UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

NORI COHAN, Derivatively on Behalf of CROWDSTRIKE HOLDINGS, INC., Plaintiff, v. GEORGE KURTZ, BURT W. PODBERE, ROXANNE S. AUSTIN, CARY J. DAVIS, JOHANNA FLOWER, SAMEER K. GANDHI, DENIS J. O'LEARY, LAURA J. SCHUMACHER, GODFREY R. SULLIVAN, and GERHARD WATZINGER, Individual Defendants, -and- CROWDSTRIKE HOLDINGS, INC., a Delaware corporation, Nominal Defendant.	Case No. 1:25-cv-00443 Public Version filed April 15, 2025

VERIFIED STOCKHOLDER DERIVATIVE COMPLAINT

Plaintiff Nori Cohan ("**Plaintiff**"), by her undersigned attorneys, derivatively on behalf of nominal defendant CrowdStrike Holdings, Inc. ("**CrowdStrike**" or the "**Company**"), files this Verified Stockholder Derivative Complaint against defendants George Kurtz ("**Kurtz**"), Burt W. Podbere ("**Podbere**"), Roxanne S. Austin ("**Austin**"), Cary J. Davis ("**Davis**"), Johanna Flower ("**Flower**"), Sameer

K. Gandhi ("**Gandhi**"), Denis J. O'Leary ("**O'Leary**"), Laura J. Schumacher ("**Schumacher**"), Godfrey R. Sullivan ("**Sullivan**"), and Gerhard Watzinger ("**Watzinger**") (collectively, the "**Individual Defendants**," and together with CrowdStrike, "**Defendants**") for violations of Section 14(a) of the Securities Exchange Act of 1934 ("**Exchange Act**"), breaches of their fiduciary duties as directors and/or officers of CrowdStrike, unjust enrichment, and for contribution under Sections 10(b) and 21D of the Exchange Act. As for Plaintiff's complaint against the Individual Defendants, Plaintiff alleges the following based upon personal knowledge as to Plaintiff and Plaintiff's own acts, and on information and belief as to all other matters, based upon, *inter alia*, the investigation conducted by and through Plaintiff's attorneys, which included, among other things, a review of the Defendants' public documents, conference calls and announcements made by Defendants, United States Securities and Exchange Commission ("**SEC**") filings, wire and press releases published by and regarding CrowdStrike, legal filings, news reports, securities analysts' reports and advisories about the Company, and information readily obtainable on the Internet. The allegations in this complaint are also based upon a review of books and records produced by the Company in response to Plaintiff's demand made pursuant to 8 *Del. C.* § 220 (the "**Section 220 Production**"). Plaintiff believes that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery

NATURE AND SUMMARY OF THE ACTION

1. Plaintiff brings this shareholder derivative action on behalf of CrowdStrike to redress breaches of fiduciary duty and other wrongdoing committed by the Individual Defendants during the period from November 29, 2023, to July 29, 2024, inclusive (the "**Relevant Period**").

2. Nominal Defendant CrowdStrike is a Delaware corporation with its principal place of business in Austin, Texas, operating as a global cybersecurity firm. Founded in 2011, CrowdStrike represents that it has "reinvented cybersecurity for the cloud era and transformed the way cybersecurity is delivered and experienced by customers."[1]

3. The Company provides cybersecurity services and technologies to a customer base that includes large corporations in industries such as airlines, banking, healthcare, and telecommunications, as well as government entities, with the stated purpose of protecting against cyber threats.[2]

4. CrowdStrike's central offering is the AI-native Falcon XDR platform ("**Falcon**"), which the Company describes as "the first, true, cloud-native platform built with artificial intelligence ('AI') at the core, capable of harnessing vast amounts

[1] *See* CrowdStrike Holdings, Inc., Annual Report (Form 10-K) (Mar. 7, 2024) ("**2024 10-K**") at 4.

[2] *See id.*

of security and enterprise data to deliver highly modular solutions through a single lightweight agent."[3]

5. CrowdStrike markets Falcon as a comprehensive platform designed to consolidate cybersecurity functions, replace outdated systems, and prevent data breaches. In the 2024 10-K, the Company asserted that Falcon "delivers a unified, modern approach that increases capability while reducing complexity and cost – all while stopping breaches," by utilizing a "single, lightweight agent" to collect and integrate enterprise data, which is then used to "train [CrowdStrike's] AI to detect and prevent threats and drive workflow automation."[4]

6. Falcon is embedded in the computer systems of CrowdStrike's customers and requires regular updates to maintain its functionality and security.

7. Throughout the Relevant Period, the Individual Defendants promoted Falcon's reliability and efficacy, repeatedly assuring investors that the Company's technology was "validated, tested, and certified." In truth, however, CrowdStrike failed to adequately develop, test, and deploy updates to Falcon, leaving the platform vulnerable to defects and errors that, as detailed below, ultimately caused millions of computers worldwide to crash and become inoperable (the "**Outage**").

[3] *Id.*

[4] *Id.*

8. The Outage occurred on July 19, 2024, when a defective update deployed by CrowdStrike triggered widespread software crashed affecting millions of Microsoft Windows devices globally, including those operated by financial institutions, government entities, and corporations. The Company subsequently disclosed that the Outage exposed affected systems to potential hacking vulnerabilities. The Outage rendered over 8.5 million devices inoperable, prompting cybersecurity experts to label it the "largest IT outage in history."[5]

9. Among other things, the Outage severely disrupted airline and airport information technology ("**IT**") systems, with the flawed Falcon update causing thousands of flight delays and cancellations as airlines struggled to maintain operations with offline computer systems.

10. Following news of the Outage, on July 19, 2024, the price of CrowdStrike's common stock declined by $38.09 per share, or approximately 11%, from a closing price of $343.05 on July 18, 2024, to $304.96 per share.

11. Further revelations emerged on July 22, 2024, when it was reported that the United States Congress had summoned Defendant Kurtz, CrowdStrike's Chief Executive Officer ("**CEO**"), to testify regarding the Outage. On the same date,

[5] Ruxandra Iordache, *Microsoft-CrowdStrike issue causes largest IT outage in history*, CNBC (July 19, 2024), https://www.cnbc.com/2024/07/19/latest-live-updates-on-a-major-it-outage-spreading-worldwide.html.

securities analysts, including those from Guggenheim and BTIG, downgraded CrowdStrike's stock rating. Additionally, *Forbes* published an article titled "The CrowdStrike Outage Is Still Impacting Airlines," reporting that "[c]ommercial airlines are still feeling the pinch days after the global CrowdStrike outage resulted in flight cancellations and travel delays for four consecutive days—and counting."[6]

12. The *Forbes* report noted that "Delta Air Lines, in particular, is the U.S. carrier still experiencing the most harmful effects from the outage," with FlightAware reporting "over 700 cancellations and 400 flight delays" as of the morning of July 22, 2024, with further increases expected.

13. As a result, on July 22, 2024, CrowdStrike's stock price fell by $41.05 per share, or approximately 13.5%, from a closing price of $304.96 on July 19, 2024, to $263.91.

14. The gravity of the situation became apparent on July 29, 2024, when it was reported that Delta Air Lines ("**Delta**") had retained prominent attorney David Boies to pursue damages from CrowdStrike arising from the Outage.

15. Following this news, on July 30, 2024, CrowdStrike's stock price dropped by $25.16 per share, or approximately 10%, from a closing price of $258.81 on July 29, 2024, to $233.65.

[6] Geoff Whitmore, *The CrowdStrike Outage Is Still Impacting Airlines*, Forbes (July 22, 2024), https://www.forbes.com/sites/geoffwhitmore/2024/07/22/the-crowdstrike-outage-is-still-impacting-airlines/.

16. During the Relevant Period, the Individual Defendants breached their fiduciary duties by personally making, or causing the Company to make, materially false and misleading statements to the investing public regarding the reliability and testing of its Falcon platform, which led to a massive global IT outage affecting millions of Microsoft Windows systems. Specifically, CrowdStrike assured investors its technology was "validated, tested, and certified," implying robust quality controls and content update procedures. However, the Outage—caused by a faulty Falcon sensor update—revealed deficient controls and inadequate testing practices.

17. CrowdStrike failed to disclose to investors that its procedures for updating Falcon were insufficiently rigorous, creating a significant risk of major disruptions. Statements from CEO George Kurtz, such as those made during a March 2024 conference call, described the platform as thoroughly "validated, tested, and certified." These claims, however, were misleading because the Company did not properly test updates before deployment, as evidenced by the mismatch in the Falcon sensor update (expecting 20 input fields but receiving 21), which triggered an out-of-bounds memory read and subsequent system crashes. This incident demonstrated that CrowdStrike's assurances about the platform's reliability and testing processes were false, leading to inflated stock prices during the Relevant Period and significant financial losses when the Outage caused the stock to plummet.

18. Moreover, during the Relevant Period, five of the Individual Defendants engaged in improper insider sales of CrowdStrike stock, collectively netting proceeds exceeding $195.5 million. Additionally, the Individual Defendants participated in or facilitated the Company's failure to adequately develop, test, and deploy updates to Falcon.

19. As a direct result of the Individual Defendants' misconduct, CrowdStrike, its CEO, and its Chief Financial Officer ("**CFO**") have been named in a federal securities class action lawsuit pending in the United States District Court for the Western District of Texas (the "**Securities Class Action**"). The Company also faces two consumer class action lawsuits in the same court (the "**Consumer Class Actions**").

20. The misconduct necessitated internal investigations, remediation of the Outage, and implementation of adequate internal controls, and resulted in losses from wasted corporate assets. These consequences will require the Company to expend millions of dollars. CrowdStrike has suffered substantial harm due to the Individual Defendants' knowing or grossly reckless breaches of fiduciary duty and related misconduct. Given the breaches of fiduciary duty by the Individual Defendants—most of whom are current directors of the Company—their collective participation in fraud and misconduct, their involvement in or facilitation of the failure to adequately develop, test, and deploy Falcon updates, the substantial

likelihood of their liability in this derivative action, Defendant Kurtz's liability in the Securities Class Action, and their lack of disinterestedness and independence, a majority of the Company's Board of Directors (the "**Board**") is incapable of impartially considering a demand to initiate litigation against themselves on behalf of the Company. Accordingly, demand upon the Board is excused as futile, and Plaintiff seeks relief on behalf of CrowdStrike to remedy the damages inflicted by the Individual Defendants' actions.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because Plaintiff's claims raise a federal question under Section 14(a) of the Exchange Act (15 U.S.C. § 78n(a)(1)), Rule 14a-9 of the Exchange Act (17 C.F.R. § 240.14a-9), Section 10(b) of the Exchange Act (15. U.S.C. § 78j(b)), and Section 21D of the Exchange Act (15 U.S.C. § 78u-4(f)). Plaintiff's claims also raise a federal question pertaining to the claims made in the Securities Class Action based on violations of the Exchange Act.

22. This Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367(a).

23. This derivative action is not a collusive action to confer jurisdiction on a court of the United States that it would not otherwise have.

24. Venue is proper in this District because the alleged misstatements and wrongs complained of herein entered this District, the Defendants have conducted business in this District, and Defendants' actions have had an effect in this District.

THE PARTIES

Plaintiff

25. Plaintiff Nori Cohan is and has continuously been a stockholder of CrowdStrike during the wrongdoing complained of herein.

Nominal Defendant

26. CrowdStrike provides cybersecurity solutions in the United States and internationally. The Company's unified platform provides cloud-delivered protection of endpoints, cloud workloads, identity, and data through a software as a service ("**SaaS**") subscription-based model. The Company offers corporate endpoint and cloud workload security, managed security, security and vulnerability management, IT operations management, identity protection, threat intelligence, data protection, SaaS security posture management, and artificial intelligence ("**AI**") powered workflow automation, and securing generative AI workload services, as well as security orchestration, automation, and response, and security information and event management, and log management services. It primarily sells subscriptions to its Falcon platform and cloud modules. CrowdStrike was incorporated in 2011 and is headquartered in Austin, Texas. CrowdStrike's flagship

product is Falcon, the cornerstone of the business, driving the bulk of the Company's revenue and market reputation.

Individual Defendants

Defendant Kurtz

27. Defendant Kurtz has served as CrowdStrike's President, CEO, and as a Company director since November 2011. He also serves as a member of the Transaction Committee. According to the Schedule 14A the Company filed with the SEC on May 6, 2024 (the "**2024 Proxy Statement**"), as of April 18, 2024, Defendant Kurtz owned 1,374,595 shares of the Company's Class A common stock. For the fiscal year ended January 31, 2024 (the "**2024 Fiscal Year**"), Defendant Kurtz received $46,983,855 in total compensation from the Company. This included $950,000 in salary, $44,090,037 in stock awards, $1,241,709 in non-equity incentive plan compensation, and $702,109 in all other compensation.

28. During the Relevant Period, while the Company's stock price was artificially inflated and before the Company's misconduct was exposed, Defendant Kurtz made the following sales of Company stock:

Date	Number of Shares	Avg. Price/Share	Proceeds
December 21, 2023	56,985	$252.94	$14,413,842
January 11, 2024	60,000	$283.16	$16,989,540
January 12, 2024	40,000	$286.10	$11,443,960
March 21, 2024	78,080	$328.38	$25,639,910
May 3, 2024	56,279	$303.57	$17,084,897
June 21, 2024	55,587	$376.16	$20,909,717
TOTALS:	**346,931**		**$106,481,866**

These insider sales, made with knowledge of material nonpublic information before the material misstatements and omissions were exposed, demonstrate Defendant Kurtz's motive in facilitating and participating in the schemes.

29. The 2024 Proxy Statement stated the following about Defendant Kurtz:

> Mr. Kurtz, 53, is one of our co-founders and has served as our Chief Executive Officer, President and a member of our board of directors since November 2011.
>
> - From October 2004 to October 2011, Mr. Kurtz served in executive roles at McAfee, Inc., a security technology company, including as Executive Vice President and Worldwide Chief Technology Officer from October 2009 to October 2011.
> - In October 1999, Mr. Kurtz founded Foundstone, Inc., a security technology company, where he served as its Chief Executive Officer until it was acquired by McAfee, Inc. in October 2004.
> - Since November 2017, he has also served as Chairman and as a board member for the CrowdStrike Foundation, a nonprofit established to support the next generation of talent and research in cybersecurity and artificial intelligence through scholarships, grants, and other activities.
> - He served on the board of directors of Hewlett Packard Enterprise, an enterprise information technology company from June 2019 until April 2023.

Defendant Podbere

30. Defendant Podbere has served as CrowdStrike's CFO since September 2015. According to the 2024 Proxy Statement, as of April 18, 2024, Defendant

Podbere owned 133,023 shares of the Company's Class A common stock. Given that the price per share of the Company's Class A common stock at the close of trading on April 18, 2024, was $294.10, Defendant Podbere owned approximately $39.1 million worth of CrowdStrike Class A common stock as of that date. For the 2024 Fiscal Year, Defendant Podbere received $20,206,385 in total compensation from the Company. This included $625,000 in salary, $18,895,730 in stock awards, $653,531 in non-equity incentive plan compensation, and $32,124 in all other compensation.

31. During the Relevant Period, while the Company's stock price was artificially inflated and before the Company's misconduct was exposed, Defendant Podbere made the following sales of Company stock:

Date	Number of Shares	Avg. Price/Share	Proceeds
December 12, 2023	41,240	$250.04	$10,311,732
December 21, 2023	22,825	$253.49	$5,785,886
March 21, 2024	26,097	$325.90	$8,505,116
April 1, 2024	64,000	$317.18	$20,299,776
May 3, 2024	15,753	$304.24	$4,792,661
May 14, 2024	12,000	$329.10	$3,949,152
May 15, 2024	12,000	$339.29	$4,071,503
May 20, 2024	5,424	$349.01	$1,893,030
May 21, 2024	6,576	$348.94	$2,294,629
June 21, 2024	11,154	$377.21	$4,207,456
TOTALS:	**217,069**		**$66,110,941**

These insider sales, made with knowledge of material nonpublic information before the material misstatements and omissions were exposed, demonstrate Podbere's motive in facilitating and participating in the schemes.

Defendant Austin

32. Defendant Austin has served as a Company director since September 2018. She also serves as Chair of the Audit Committee. According to the 2024 Proxy Statement, as of April 18, 2024, Defendant Austin owned 15,919 shares of the Company's Class A common stock. Given that the price per share of the Company's Class A common stock at the close of trading on April 18, 2024, was $294.10, Defendant Austin owned approximately $4.7 million worth of CrowdStrike Class A common stock as of that date. For the 2024 Fiscal Year, Defendant Austin received $334,668 in total compensation from the Company. This included $65,000 in fees earned or paid in cash, $249,867 in stock awards, and $19,801 in all other compensation.

33. During the Relevant Period, while the Company's stock price was artificially inflated and before the Company's misconduct was exposed, Defendant Austin made the following sales of Company stock:

Date	Number of Shares	Avg. Price/Share	Proceeds
June 27, 2024	10,000	$390.01	$3,900,100
June 28, 2024	5,000	$391.01	$1,955,050
TOTALS:	**15,000**		**$5,855,150**

These insider sales, made with knowledge of material nonpublic information before

the material misstatements and omissions were exposed, demonstrate Austin's motive in facilitating and participating in the schemes.

Defendant Davis

34. Defendant Davis has served as a Company director since July 2013. He also serves as a member of the Compensation Committee. According to the 2024 Proxy Statement, as of April 18, 2024, Defendant Davis owned 18,418 shares of the Company's Class A common stock. Given that the price per share of the Company's Class A common stock at the close of trading on April 18, 2024, was $294.10, Defendant Davis owned approximately $5.4 million worth of CrowdStrike Class A common stock as of that date. For the 2024 Fiscal Year, Defendant Davis received $299,367 in total compensation from the Company. This included $49,500 in fees earned or paid in cash and $249,867 in stock awards.

Defendant Flower

35. Defendant Flower has served as a Company director since January 2023. According to the 2024 Proxy Statement, as of April 18, 2024, Defendant Flower owned 80,883 shares of the Company's Class A common stock. Given that the price per share of the Company's Class A common stock at the close of trading on April 18, 2024, was $294.10, Defendant Flower owned approximately $23.8 million worth of CrowdStrike Class A common stock as of that date. For the 2024 Fiscal Year, Defendant Flower received $315,927 in total compensation from the Company. This

included $40,000 in fees earned or paid in cash, $249,867 in stock awards, and $26,060 in all other compensation.

Defendant Gandhi

36. Defendant Gandhi has served as a Company director since August 2013. He also serves as Chair of the Compensation Committee and as a member of the Transaction Committee. According to the 2024 Proxy Statement, as of April 18, 2024, Defendant Gandhi owned 910,641 shares of the Company's Class A common stock. Given that the price per share of the Company's Class A common stock at the close of trading on April 18, 2024, was $294.10, Defendant Gandhi owned approximately $267.8 million worth of CrowdStrike Class A common stock as of that date. For the 2024 Fiscal Year, Defendant Gandhi received $309,450 in total compensation from the Company. This included $59,583 in fees earned or paid in cash and $249,867 in stock awards.

37. During the Relevant Period, while the Company's stock price was artificially inflated and before the Company's misconduct was exposed, Defendant Gandhi made the following sales of Company stock:

Date	Number of Shares	Avg. Price/Share	Proceeds
January 3, 2024	15,000	$240.13	$3,601,995
April 3, 2024	15,000	$317.18	$4,757,625
July 1, 2024	15,000	$382.02	$5,730,285
TOTALS:	**45,000**		**$14,089,905**

These insider sales, made with knowledge of material nonpublic information before

the material misstatements and omissions were exposed, demonstrate Gandhi's motive in facilitating and participating in the schemes.

Defendant O'Leary

38. Defendant O'Leary has served as a Company director since December 2011. He also serves as Chair of the Nominating and Corporate Governance Committee. According to the 2024 Proxy Statement, as of April 18, 2024, Defendant O'Leary owned 12,656 shares of the Company's Class A common stock. Given that the price per share of the Company's Class A common stock at the close of trading on April 18, 2024, was $294.10, Defendant O'Leary owned approximately $3.7 million worth of CrowdStrike Class A common stock as of that date. For the 2024 Fiscal Year, Defendant O'Leary received $299,867 in total compensation from the Company. This included $50,000 in fees earned or paid in cash and $249,867 in stock awards.

39. During the Relevant Period, while the Company's stock price was artificially inflated and before the schemes were exposed, Defendant O'Leary made the following sales of Company stock:

Date	Number of Shares	Avg. Price/Share	Proceeds
December 7, 2023	4,040	$238.40	$963,136
June 10, 2024	5,300	$381.45	$2,021,685
TOTALS:	**9,340**		**$2,984,821**

These insider sales, made with knowledge of material nonpublic information before the material misstatements and omissions were exposed, demonstrate O'Leary's motive in facilitating and participating in the schemes.

Defendant Schumacher

40. Defendant Schumacher has served as a Company director since November 2020. She also serves as a member of the Nominating and Corporate Governance Committee. According to the 2024 Proxy Statement, as of April 18, 2024, Defendant Schumacher owned 6,041 shares of the Company's Class A common stock. Given that the price per share of the Company's Class A common stock at the close of trading on April 18, 2024, was $294.10, Defendant Schumacher owned approximately $1.8 million worth of CrowdStrike Class A common stock as of that date. For the 2024 Fiscal Year, Defendant Schumacher received $294,867 in total compensation from the Company. This included $45,000 in fees earned or paid in cash and $249,867 in stock awards.

Defendant Sullivan

41. Defendant Sullivan has served as a Company director since December 2017. He also serves as a member of the Audit Committee. According to the 2024 Proxy Statement, as of April 18, 2024, Defendant Sullivan owned 78,887 shares of the Company's Class A common stock. Given that the price per share of the Company's Class A common stock at the close of trading on April 18, 2024, was

$294.10, Defendant Sullivan owned approximately $23.2 million worth of CrowdStrike Class A common stock as of that date. For the 2024 Fiscal Year, Defendant Sullivan received $299,867 in total compensation from the Company. This included $50,000 in fees earned or paid in cash and $249,867 in stock awards.

Defendant Watzinger

42. Defendant Watzinger has served as a Company director since April 2012. He also serves as a member of the Audit Committee, Nominating and Corporate Governance Committee, and Transaction Committee. According to the 2024 Proxy Statement, as of April 18, 2024, Defendant Watzinger owned 53,990 shares of the Company's Class A common stock. Given that the price per share of the Company's Class A common stock at the close of trading on April 18, 2024, was $294.10, Defendant Watzinger owned approximately $15.9 million worth of CrowdStrike Class A common stock as of that date. For the 2024 Fiscal Year, Defendant Watzinger received $374,668 in total compensation from the Company. This included $105,000 in fees earned or paid in cash, $249,867 in stock awards, and $19,801 in all other compensation.

FIDUCIARY DUTIES OF THE INDIVIDUAL DEFENDANTS

43. By reason of their positions as officers, directors, and/or fiduciaries of the Company and because of their ability to control the business and corporate affairs

of the Company, the Individual Defendants owed the Company and its shareholders fiduciary obligations of trust, loyalty, good faith, and due care, and were and are required to use their utmost ability to control and manage the Company in a fair, just, honest, and equitable manner. The Individual Defendants were and are required to act in furtherance of the best interests of the Company and its shareholders so as to benefit all shareholders equally.

44. Each director and/or officer of the Company owes to CrowdStrike and its shareholders the fiduciary duty to exercise good faith and diligence in the administration of the Company and in the use and preservation of its property and assets and the highest obligations of fair dealing.

45. The Individual Defendants, because of their positions of control and authority as directors and/or officers of the Company, were able to and did, directly and/or indirectly, exercise control over the wrongful acts complained of herein or aided and abetted the same.

46. To discharge their duties, the officers and/or directors of the Company were required to exercise reasonable and prudent supervision over the management, policies, controls, and operations of the Company.

47. As senior executive officers and/or directors of a publicly-traded company whose common stock was registered with the SEC pursuant to the Exchange Act and traded on the NASDAQ, the Individual Defendants at

CrowdStrike had a duty to prevent and not to effect the dissemination of inaccurate and untruthful information with respect to the Company's financial condition, performance, growth, operations, financial statements, business, products, management, earnings, internal controls, and present and future business prospects, including the dissemination of false information regarding the Company's business, prospects, and operations, and had a duty to cause the Company to disclose in its regulatory filings with the SEC all those facts described in this Complaint that it failed to disclose, so that the market price of the Company's common stock would be based upon truthful and accurate information. Further, they had a duty to ensure the Company remained in compliance with all applicable laws.

48. To discharge their duties, the officers and/or directors of the Company were required to exercise reasonable and prudent supervision over the management, policies, practices, and internal controls of the Company. By virtue of such duties, the officers and/or directors of the Company were required to, among other things, ensure that the Company was operated in a diligent, honest, and prudent manner in accordance with the laws and regulations of Delaware, Texas, and the United States, and, pursuant to CrowdStrike's own Code of Ethics & Business Conduct (the "**Code of Ethics**"):

> conduct the affairs of the Company in an efficient, business-like manner so as to make it possible to provide the highest quality performance of its business, to avoid

> wasting the Company's assets, and to maximize the value of the Company's stock;
>
> remain informed as to how the Company conducted its operations, and, upon receipt of notice or information of imprudent or unsound conditions or practices, to make reasonable inquiry in connection therewith, and to take steps to correct such conditions or practices;
>
> establish and maintain systematic and accurate records and reports of the business and internal affairs of the Company and procedures for the reporting of the business and internal affairs to the Board and to periodically investigate, or cause independent investigation to be made of, said reports and records;
>
> maintain and implement an adequate and functioning system of internal legal, financial, and management controls, such that the Company's operations would comply with all applicable laws and the Company's financial statements and regulatory filings filed with the SEC and disseminated to the public and the Company's shareholders would be accurate;
>
> exercise reasonable control and supervision over the public statements made by the Company's officers and employees and any other reports or information that the Company was required by law to disseminate;
>
> refrain from unduly benefiting themselves and other Company insiders at the expense of the Company; and
> examine and evaluate any reports of examinations, audits, or other financial information concerning the financial affairs of the Company and to make full and accurate disclosure of all material facts concerning, *inter alia*, each of the subjects and duties set forth above.

49. Under the heading "Insider Trading," the Code of Ethics states the following:

> Insider trading violates this Code and the law, and may result in substantial civil and criminal penalties, including the possibility of a jail sentence.
>
> Buying or selling stock while in possession of material non-public information or passing such information along to others so that they may buy or sell stock, constitutes illegal insider trading.
>
> CrowdStrike shares non-public information with CrowdStrikers to successfully carry out our business. You may also inadvertently learn non-public information – for example by overhearing a conversation.

50. Each of the Individual Defendants further owed to the Company and its shareholders a duty of loyalty requiring that he or she favor the Company's interest and that of its shareholders over his or her own interest while conducting the affairs of the Company and refrain from using his or her position, influence, or knowledge of the affairs of the Company to gain personal advantage.

51. Because of their advisory, executive, managerial, and directorial positions with the Company, each of the Individual Defendants had access to adverse, non-public information about the Company.

52. The Individual Defendants, because of their positions of control and authority, were able to and did, directly or indirectly, exercise control over the wrongful acts complained of herein, as well as the contents of the various public statements issued by the Company.

CONSPIRACY, AIDING AND ABETTING, AND CONCERTED ACTION

53. In committing the wrongful acts alleged herein, the Individual Defendants have pursued, or joined in the pursuit of, a common course of conduct, and have acted in concert with and conspired with one another in furtherance of their wrongdoing. The Individual Defendants caused the Company to conceal the true facts as alleged herein. The Individual Defendants further aided and abetted and/or assisted each other in breaching their respective duties.

54. The purpose and effect of the conspiracy, common enterprise, and/or common course of conduct was, among other things, to: (i) facilitate and disguise the Individual Defendants' violations of law, including breaches of fiduciary duty, unjust enrichment, and violations of the Exchange Act; (ii) conceal adverse information concerning the Company's operations, financial condition, legal compliance, future business prospects, and internal controls; and (iii) artificially inflate the Company's stock price.

55. The Individual Defendants accomplished their conspiracy, common enterprise, and/or common course of conduct by causing the Company to purposefully or recklessly conceal material facts, fail to correct such misrepresentations, and violate applicable laws. In furtherance of this plan, conspiracy, and course of conduct, the Individual Defendants collectively and individually took the actions set forth herein. Because the actions described herein

occurred under the authority of CrowdStrike's board of directors, each of the Individual Defendants who was a director of CrowdStrike was a direct, necessary, and substantial participant in the conspiracy, common enterprise, and/or common course of conduct complained of herein.

56. Each of the Individual Defendants aided and abetted and rendered substantial assistance in the wrongs complained of herein. In taking such actions to substantially assist the commission of the wrongdoing complained of herein, each of the Individual Defendants acted with actual or constructive knowledge of the primary wrongdoing, either took direct part in or substantially assisted with the accomplishment of that wrongdoing, and was or should have been aware of his or her overall contribution to and in furtherance of the wrongdoing.

57. At all times relevant hereto, each of the Individual Defendants was the agent of each of the other Individual Defendants and/or of the Company and was at all times acting within the course and scope of such agency.

Duties Pursuant to the Company's Corporate Governance Guidelines

58. CrowdStrike represents that its Corporate Governance Guidelines were adopted "to promote the effective functioning of the Board and its committees, to promote the interests of stockholders, and to ensure a common set of expectations as to how the Board, its various committees, individual directors, and management should perform their functions."

59. Under the heading "Director Responsibilities," the Corporate Governance Guidelines state:

> The Board acts as the ultimate decision-making body of the Company and advises and oversees management, who are responsible for the day-to-day operations and management of the Company. In fulfilling this role, each director must act in what he or she reasonably believes to be in the best interests of the Company and must exercise his or her business judgment.

60. Under a section titled "Board Committees," the Corporate Governance Guidelines describe the role of the Audit Committee as:

> The Audit Committee shall generally be responsible for overseeing the integrity of the Company's financial statements, its independent auditor, its internal audit function and compliance by the Company with legal and regulatory requirements, and overseeing the Company's Policy for Reporting Concerns to Accounting, Auditing and Ethical Violations (Whistleblower Policy).

61. In violation of the Code of Ethics and Corporate Governance Guidelines, the Individual Defendants conducted little, if any, oversight of the Company's engagement in the Individual Defendants' schemes to cause the Company to engage in misconduct with regard to testing of updates to the Falcon platform, which ultimately led to the Outage; issue materially false and misleading statements to the public; and facilitate and disguise the Individual Defendants' violations of law, including breaches of fiduciary duty, unjust enrichment, and violations of the Exchange Act. Also, in violation of the Code of Ethics, the Individual

Defendants failed to: (i) maintain internal controls; (ii) comply with laws and regulations; (iii) conduct business in an honest and ethical manner; and (iv) properly report violations of the Codes of Ethics.

CROWDSTRIKE'S AUDIT COMMITTEE CHARTER

62. The Company also maintains an Audit Committee Charter (the "**Audit Committee Charter**"). According to the Audit Committee Charter, the purpose of the Audit Committee is to, *inter alia*:

> The Audit Committee (the 'Committee') was created by the Board of Directors (the 'Board') to: assist the Board in its oversight of: the integrity of the Company's financial statements and internal controls; the qualifications, independence and performance of the Company's independent auditor; the performance of the Company's internal audit function; the Company's compliance with legal and regulatory requirements; and prepare the Committee report that the Securities and Exchange Commission (the 'SEC') rules require to be included in the Company's annual proxy statement.

63. The Audit Committee Charter, under the heading "Responsibilities," states that:

> The basic responsibility of the members of the Committee is to exercise their business judgment to act in what they reasonably believe to be in the best interests of the Company and its shareholders. In discharging that obligation, members should be entitled to rely on the honesty and integrity of the Company's senior executives and its outside advisors and auditors, to the fullest extent permitted by law. In addition to any other responsibilities which may be assigned from time to time by the Board, the Committee is responsible for the following matters.

64. Under the same heading, in the subsection titled "*Financial Statements; Disclosure and Other Risk Management and Compliance Matters*," the Audit Committee Charter states that the responsibilities of the Audit Committee include the following:

- The Committee shall review the Company's policies and practices with respect to risk assessment and risk management, including the Company's policies and practices pertaining to financial accounting, investment, tax, and cybersecurity matters, and shall discuss with management the Company's major financial risk exposures and the steps that have been taken to monitor and control such exposures.

- The Committee shall establish procedures for:

  - the receipt, retention and treatment of complaints received by the Company regarding accounting, internal accounting controls or auditing matters, and

  - the confidential, anonymous submission by employees of the Company of concerns regarding questionable accounting or auditing matters.

- The Committee shall prepare the Committee report that the SEC rules require to be included in the Company's annual proxy statement.

- The Committee shall review the Company's compliance with laws and regulations, including major legal and regulatory initiatives. The Committee shall also review any major litigation or investigations against the Company that may have a material impact on the Company's financial statements. The Committee shall meet and discuss these matters with

> management and others as appropriate, including the General Counsel of the Company.

65. Under the same heading, in the subsection titled "*Reporting to the Board*," the Audit Committee Charter states that the responsibilities of the Committee are as follows:

> - The Committee shall report to the Board periodically. This report shall include a review of any issues that arise with respect to the quality or integrity of the Company's financial statements, the Company's compliance with legal or regulatory requirements, the independence and performance of the Company's independent auditor, the performance of the internal audit function, and any other matters that the Committee deems appropriate or is requested to include by the Board.
>
> - At least annually, the Committee shall evaluate its own performance and report to the Board on such evaluation.
>
> - The Committee shall review and assess the adequacy of this charter annually and recommend any proposed changes to the Board.

66. In violation of the Audit Committee Charter, Defendants Austin, Sullivan, and Watzinger (collectively the "**Audit Committee Defendants**"), as members of the Company's Board, conducted little, if any, oversight of the Company's engagement in the Individual Defendants' schemes to cause the Company to participate in inadequate testing that resulted in the Outage; issue materially false and misleading statements to the public; and facilitate and disguise

the Individual Defendants' violations of law, including breaches of fiduciary duty, unjust enrichment, and violations of the Exchange Act. Moreover, in violation of the Audit Committee Charter, the Audit Committee Defendants failed to maintain the accuracy of the Company's records and reports, comply with laws and regulations, act in good faith and diligence without misstating, misrepresenting, or omitting material facts, and properly report violations of the Audit Committee Charter.

SUBSTANTIVE ALLEGATIONS

Background

67. CrowdStrike asserts that it revolutionized cybersecurity for the "cloud" era, reshaping how it is provided and perceived by its clients. The Company serves major corporations across multiple sectors, including airlines, banks, hospitals, telecommunications firms, and government agencies.

68. The Company claims its primary focus is developing platforms to prevent data breaches. Its flagship product, the Falcon platform, is marketed as the pioneering cloud-native solution with AI at its core. CrowdStrike states that Falcon leverages vast security and enterprise data to offer modular solutions via a single lightweight agent.

69. CrowdStrike markets Falcon as the leading platform for consolidating cybersecurity, designed specifically to halt data breaches. The Company's 2024 10-K states that Falcon unifies security and IT by replacing outdated products and

disjointed platforms, delivering a streamlined, modern approach that enhances capabilities while cutting complexity and costs—all while preventing breaches. Falcon's lightweight agent reportedly gathers and integrates enterprise-wide data, which CrowdStrike uses to train its AI to identify and thwart threats, automating workflows to give security teams a rapid advantage against adversaries.

70. Embedded in customer computers, the Falcon platform requires regular updates. CrowdStrike delivers these updates in at least two forms: (1) "Sensor Content" updates that modify Falcon's sensor directly; and (2) "Rapid Response Content" updates that adjust sensor behavior to detect threats. As a cloud-based, automated system, Falcon employs continuous integration and delivery, meaning updates roll out simultaneously to many customers at scale.

The Outage

71. Shortly after midnight on July 19, 2024, CrowdStrike issued a defective Rapid Response Content update for Falcon, triggering widespread technology failures across millions of Microsoft Windows devices. As an endpoint system, Falcon pushed this update to thousands of individual computer endpoints simultaneously, even when customers did not enable automatic update settings.[7] The

[7] CrowdStrike eventually admitted that it should have provided customers with "control over the deployment of Rapid Response Content updates" so that they could "chose where and when Rapid Response Content updates are deployed." *See* CrowdStrike, *External Technical Root Cause Analysis – Channel File 291* (Aug. 6, 2024), https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf.

update's faulty data file caused an out-of-bounds exception in Windows, crashing numerous endpoints.

72. The CrowdStrike Outage affected roughly 8.5 million Windows devices, earning a reputation as possibly the largest IT outage ever recorded. It disrupted government agencies and major corporations alike, grounding airline flights, disabling emergency 911 services, and crashing 15,000 servers at just one hospital, impacting 40,000 of its 150,000 computers.

73. Although CrowdStrike attempted to retract the update shortly after deployment, the damage was irreversible. Affected computers shut down, endlessly attempting to reboot and displaying the infamous "Blue Screen of Death." The situation worsened as each endpoint required manual restarts to recover.

74. In a July 19, 2024 blog post about "The Impact of Faulty EDR And ELAM Drivers," CrowdStrike noted that the Outage appeared "to be linked to the CrowdStrike Falcon Endpoint Detection Response (EDR) agent, specifically its Early Launch Anti-Malware (ELAM) driver."[8] Although it was still unclear at that time what had caused the Outage, the Company stated:

[8] CrowdStrike noted that "ELAM driver signing is exclusive to companies [like CrowdStrike] that create EDR products, with Microsoft granting access only after a degree of trust and verification." As one of these trusted companies, CrowdStrike was required to submit any deep-system "kernel-level" programming and data for rigorous testing and verification for deployment. Although the Company claimed that it complied with these operating system requirements, it would ultimately become clear that CrowdStrike had not submitted its solutions to the promised rigorous testing.

> This incident highlights the critical need for stringent testing and quality assurance in cybersecurity products, especially those operating at the kernel level. EDR and ELAM driver updates must undergo extensive validation to prevent catastrophic failures that can cripple businesses worldwide.

75. On the same day, CrowdStrike posted a blog titled "Our Statement on Today's Outage," in which Defendant Kurtz apologized, saying: "I want to sincerely apologize directly to all of you for today's outage. All of CrowdStrike understands the gravity and impact of the situation." The Company also cautioned that malicious actors were exploiting the Outage to target CrowdStrike customers, with Kurtz urging vigilance and reliance on official CrowdStrike channels for updates.

76. Two leaders from Congress's Homeland Security Committee wrote to Defendant Kurtz, emphasizing the Outage's severity: "In less than one day, we have seen major impacts to key functions of the global economy, including aviation, healthcare, banking, media, and emergency services."

77. The core issue behind the Outage proved to be a flaw in the Content Validator Tool, which failed to catch problematic content in the update (specifically in Channel File 291). The Content Validator, in the context of CrowdStrike's operations, refers to an automated tool or process designed to check and validate updates—specifically, the Rapid Response Content updates for the Falcon sensor platform—before they are deployed to customer systems. The Content Validator Tool's primary purpose is to ensure that the content being pushed out is safe,

functional, and compatible with the existing software environment, ideally catching errors that could lead to system instability or crashes.

78. This update, however, included a mismatch where the sensor expected 20 input fields, but the update provided 21, leading to an unhandled exception. While CrowdStrike claimed it conducted stress testing and validation for new Template Types, the Company actually relied heavily on the Content Validator Tool's automated checks rather than subjecting Rapid Response Content to the same rigorous, multi-stage testing as the Company's Sensor Content updates. This lighter testing approach for Rapid Response Content, which is meant to deploy quickly to address emerging threats, assumed the validator would catch issues based on prior successful deployments. However, a bug in the validator allowed the faulty update to pass through undetected.

79. Additionally, CrowdStrike did not implement a staggered deployment strategy for this update, meaning it rolled out to all affected systems simultaneously rather than to a smaller test group first.[9] This lack of a "canary" or phased rollout prevented the Company from identifying the issue on a limited scale before it crashed millions of devices globally. Experts have noted that even basic integration or deployment testing on a variety of real-world configurations could have exposed

[9] The Company eventually admitted that updates "should be deployed in a staged rollout[,]" explaining that "[s]tagged deployment mitigates impact if a new [update] causes failure such as system crashes[.]" *Id.*

the problem, suggesting that CrowdStrike's testing was overly reliant on theoretical validation rather than practical, end-to-end checks.

80. In summary, CrowdStrike's errors included over-reliance on a flawed automated validator, insufficient real-world testing of Rapid Response Content updates, and the absence of a gradual deployment to catch issues early. Following the incident, the Company pledged to enhance testing with local developer checks, stress testing, and a staged rollout approach to prevent such failures in the future. Nevertheless, the damage was done and, as detailed herein, would have been avoidable had management and the Board exercised the degree of care required to operate an international cybersecurity firm.

The Company Was Aware of the Risks of Errors with Falcon Content Updates

81. Throughout the Relevant Period, Defendants knew or should have known that inadequate development, testing, and validation processes posed a significant risk of releasing flawed content updates with severe defects or bugs. They also understood that such flaws could trigger widespread outages across customer systems. Yet, CrowdStrike neglected smaller-scale testing for Falcon updates, ensuring that any errors would simultaneously crash all customer systems.

82. Post-Outage, cybersecurity expert Eric O'Neill told CNBC that CrowdStrike's practice of rolling out updates to all users at once was flawed: "Send it to one group and test it. There are levels of quality control it should go through."

Peter Avery of Visual Edge IT added that the update "should have been tested in sandboxes, in many environments before it went out," suggesting a lack of proper checks could stem from a single person's error.

83. A July 23, 2024, article in *The Verge* also criticized CrowdStrike, stating that gradual rollouts are standard practice and that proper testing with a small user group could have limited the damage to a minor issue rather than a global tech catastrophe.

84. Marcus Merrell of Sauce Labs agreed, stressing, in a July 29, 2024, CSOOnline.com article, that interconnected software demands gradual rollouts: "You must slow-roll the release over hours or days, rather than risk crippling the entire planet with one large update."

85. On July 30, 2024, SentinelOne's CEO was asked about the CrowdStrike faulty update and stated:

> I haven't seen anybody update the kernel in such a way [as CrowdStrike did] – and definitely not in a way that doesn't go through customer approval, as well. I mean, the other part here is, it's not just Microsoft in the process. It's customers. You're [supposed to be] giving customers the ability to control what's deployed, when it's deployed, what version is deployed, rollback capabilities, gradual rollout, phased deployments. All of those are kind of table stakes. So to see that with one push [of a] button, this gets immediately sent globally, causing the biggest IT security outage in history – it's not just a mistake. It's just architecture.

86. CrowdStrike's SEC filings acknowledged risks of defects in its complex cloud-native platform, admitting that undetected errors could emerge post-deployment, impacting Falcon's performance. The 2024 10-K noted customers' low tolerance for interruptions and referenced a prior April 2024 Linux update that crashed systems, taking nearly five days to fix—evidence the company knew the potential consequences of faulty updates.

87. Post-Outage, CrowdStrike pledged to improve system monitoring, phase rollouts, and give customers more control over Rapid Response Content updates to prevent simultaneous failures. These commitments suggest the Company could have implemented better testing procedures beforehand but failed to do so.

88. On August 10, 2024, CrowdStrike's president accepted the Pwnie Award for "most epic fail," admitting, "We got this horribly wrong… it's super important to own it when you do things horribly wrong."

Fallout From the CrowdStrike Outage

89. The outage significantly harmed CrowdStrike. On July 30, 2024, investors filed a Securities Class Action in this Court, alleging federal securities law violations by the Company and Defendants Kurtz and Podbere for misrepresenting testing procedures and update efficacy.

90. That same day, CNN reported that Delta had hired David Boies' law firm to pursue damages from CrowdStrike and Microsoft, estimating costs between $325 million and $475 million.

91. Delta suffered profoundly from the CrowdStrike Outage, canceling over 5,000 flights between July 19 and July 25, 2024. As alleged in Delta's lawsuit against CrowdStrike, the Outage "disabled most of Delta's computers running on a Microsoft Windows operating system ('Microsoft OS'), crippled Delta's operations for several days, forced thousands of flight cancellations and delays, and adversely affected more than a million Delta customers."[10]

92. Unlike other airlines that resumed normal operations relatively quickly, Delta's customers faced prolonged disruptions, with at least 500,000 passengers stranded nationwide due to repeated flight delays and cancellations. Among other things, the Outage incapacitated Delta's crew-tracking system, preventing the airline from locating pilots and flight attendants to reschedule flights—a problem that persisted even after systems began recovering.

93. Each affected Delta computer reportedly needed to be remediated manually rather than being fixed remotely. Ultimately, Delta's IT team manually repaired over 1,500 crashed systems and reset 40,000 affected servers.

[10] *See Delta Air Lines, Inc. v. CrowdStrike, Inc.*, C.A. No. 24CV013621 (Ga. Super. Oct. 25, 2024), Complaint at 2.

94. Delta estimates the Outage caused a $380 million revenue loss from refunds and customer compensation in cash and SkyMiles, plus $170 million in additional recovery costs, including reimbursements and support for affected crew members.

95. CrowdStrike also faces two Consumer Class Actions in this Court, claiming negligence in deploying the faulty Falcon update.

96. On August 29, 2024, *The Wall Street Journal* reported that CrowdStrike slashed its revenue forecast, citing over $60 million in customer incentives and a nearly 23% stock drop since the Outage, with shares falling another 4% after hours. The article highlighted Delta's $500 million loss and its retention of David Boies to seek compensation for its staggering losses.

The Individual Defendants' False and Misleading Statements

November 29, 2023 Earnings Call & Form 10-Q

97. On November 29, 2023, CrowdStrike hosted an earnings call with analysts and investors to discuss the Company's financial results for the third quarter of the 2024 Fiscal Year. During the call, Defendant Kurtz touted the capabilities of Falcon, representing that it "has made cybersecurity easy and effective for small businesses to the world's largest enterprises" and that the "drumbeat of innovation was loud and clear with multiple releases and announcements showcasing CrowdStrike as the XDR leader, including the Falcon platform Raptor release." He

also stated that "from hygiene to patching, Falcon for IT lets customers consolidate multiple use cases and replace legacy products with our single-agent architecture," and boasted of CrowdStrike's "new Falcon Data Protection module that liberates customers from legacy [data loss prevention] products with modern, frictionless data security."

98. Also on November 29, 2023, CrowdStrike filed its quarterly report on Form 10-Q with the SEC for the quarterly period ended October 31, 2023 (the "**3Q24 10-Q**"). Attached to the 3Q24 10-Q were certifications made pursuant to the Sarbanes-Oxley Act of 2002 ("**SOX**") and signed by Defendants Kurtz and Podbere certifying that the 3Q24 10-Q "fully complies with the requirements of Section 13(a) or 15(d) of the [Exchange Act]" and that the "information contained in the [3Q24 10-Q] fairly presents, in all material respects, the financial condition and results of operations of [the Company]."

99. With respect to risk factors to CrowdStrike's business, the 3Q24 10-Q stated the following, in relevant part:

> If our solutions fail or are perceived to fail to detect or prevent incidents or have or are perceived to have defects, errors, or vulnerabilities, our brand and reputation would be harmed, which would adversely affect our business and results of operations.
>
> Real or perceived defects, errors or vulnerabilities in our Falcon platform and cloud modules, the failure of our platform to detect or prevent incidents, including advanced and newly developed attacks, misconfiguration

of our solutions, or the failure of customers to take action on attacks identified by our platform could harm our reputation and adversely affect our business, financial position and results of operations.

We rely on third-party data centers, such as Amazon Web Services, and our own colocation data centers to host and operate our Falcon platform, and any disruption of or interference with our use of these facilities may negatively affect our ability to maintain the performance and reliability of our Falcon platform which could cause our business to suffer.

Our customers depend on the continuous availability of our Falcon platform. We currently host our Falcon platform and serve our customers using a mix of third-party data centers, primarily Amazon Web Services, Inc., or AWS, and our data centers, hosted in colocation facilities. Consequently, we may be subject to service disruptions as well as failures to provide adequate support for reasons that are outside of our direct control. We have experienced, and expect that in the future we may experience interruptions, delays and outages in service and availability from time to time due to a variety of factors, including infrastructure changes, human or software errors, website hosting disruptions and capacity constraints.

The following factors, many of which are beyond our control, can affect the delivery, availability, and the performance of our Falcon platform:

***

•errors, defects or performance problems in our software, including third-party software incorporated in our software;
•improper deployment or configuration of our solutions;
•the failure of our redundancy systems, in the event of a service disruption at one of our data centers, to provide

> failover to other data centers in our data center network; and
> •the failure of our disaster recovery and business continuity arrangements.
>
> The adverse effects of any service interruptions on our reputation, results of operations, and financial condition may be disproportionately heightened due to the nature of our business and the fact that our customers have a low tolerance for interruptions of any duration. Interruptions or failures in our service delivery could result in a cyberattack or other security threat to one of our customers during such periods of interruption or failure. Additionally, interruptions or failures in our service could cause customers to terminate their subscriptions with us, adversely affect our renewal rates, and harm our ability to attract new customers. Our business would also be harmed if our customers believe that a cloud-based SaaS-delivered endpoint security solution is unreliable. While we do not consider them to have been material, we have experienced, and may in the future experience, service interruptions and other performance problems due to a variety of factors. The occurrence of any of these factors, or if we are unable to rapidly and cost-effectively fix such errors or other problems that may be identified, could damage our reputation, negatively affect our relationship with our customers or otherwise harm our business, results of operations and financial condition.

March 5, 2024 Earnings Call

100. On March 5, 2024, CrowdStrike hosted an earnings call with analysts and investors to discuss its financial results for the 2024 Fiscal Year. During the call, Defendant Kurtz continued to boast of Falcon's capabilities, representing that it "is validated, tested and certified." He also emphasized the Company's "execution and discipline across the business."

March 7, 2024 Form 10-K

101. On March 7, 2024, CrowdStrike filed the 2024 10-K with the SEC. Defendants Kurtz, Podbere, Watzinger, Davis, O'Leary, Sullivan, Flower, Schumacher, Austin, and Gandhi signed the 2024 10-K. Attached to the 2024 10-K were SOX certifications made and signed by Defendants Kurtz and Podbere certifying that the 2024 10-K "fully complies with the requirements of Section 13(a) or 15(d) of the [Exchange Act]" and that the "information contained in the [2024 10-K] fairly presents, in all material respects, the financial condition and results of operations of [the Company."

102. The 2024 10-K represented the following about the alleged "key benefits" of CrowdStrike's business approach and the Falcon platform:

> We offer our customers compelling business value that includes ease of adoption, rapid time-to-value, superior efficacy rates in detecting threats and preventing breaches, and reduced total cost of ownership by consolidating legacy, siloed, and multi-agent security products in a single solution. We also allow thinly-stretched security organizations to automate previously manual tasks, freeing them to focus on their most important objectives. With the Falcon platform, organizations can transform how they combat threats, transforming from slow, manual, and reactionary to fast, automated, and predictive, while gaining visibility across the threat lifecycle.
>
> Key benefits of our approach and the CrowdStrike Falcon platform include:
>
> * * *

•High Efficacy, Low False Positives: The vast telemetry of the Security Cloud and the best practices employed in continually training our AI models results in industry-leading efficacy rates and low false positives.

•Consolidation of Siloed Products: Integrating and maintaining numerous security products creates blind spots that attackers can exploit, is costly to maintain and negatively impacts user performance. Our cloud-native platform approach gives customers a unified approach to address their most critical areas of risk seamlessly. We empower customers to rapidly deploy and scale industry leading technologies across endpoint detection and response ("EDR") and Extended Detection and Response ("XDR"), Identity Threat Protection, Threat Intelligence, Exposure Management, Cloud Security, Application Security Posture Management, Next- Generation SIEM and Modern Log Management, and IT Automation from a single platform.

•Reducing Agent Bloat: Our single intelligent lightweight agent enables frictionless deployment of our platform at scale, enabling customers to rapidly adopt our technology across any type of workload running on a variety of endpoints. The agent is nonintrusive to the end user, requires no reboots and continues to protect the endpoint and track activity even when offline. Through our single lightweight agent approach, customers can adopt multiple platform modules to address their critical areas of risk without burdening the endpoint with multiple agents. Legacy approaches often require multiple agents as they layer on new capabilities. This can severely impact user performance and create barriers to security.

•Rapid Time to Value: Our cloud-native platform was built to rapidly scale industry leading protection across the entire enterprise, eliminating lengthy implementation periods and professional services engagements that next-gen and legacy competitors may require. Our single agent,

collect once and re-use many times approach enables us to activate new modules in real time.

•Elite Security Teams as a Force Multiplier: As adversaries continue to employ sophisticated malwareless attacks that exploit user credentials and identities, automation and autonomous security are no longer sufficient on their own. Stopping today's sophisticated attacks requires a combination of powerful automation and elite threat hunting. Falcon Complete provides a comprehensive monitoring, management, response, and remediation solution to our customers and is designed to bring enterprise level security to companies that may lack enterprise level resources.

CrowdStrike Falcon OverWatch, part of CrowdStrike Counter Adversary Operations, combines world-class human intelligence from our elite security experts with the power of the Falcon platform. OverWatch is a force multiplier that extends the capabilities and improves the productivity of our customers' security teams. Because our world-class team can see attacks across our entire customer base, their expertise is enhanced by their constant visibility into the threat landscape. Additionally, the insights of our OverWatch team can then be leveraged by the Falcon platform to further enhance its autonomous capabilities, creating a positive feedback loop for our customers.

•Alleviating the Skills Shortage through Automation: CrowdStrike automates manual tasks to free security teams to focus on their most important job – stopping the breach. Our Falcon Fusion capability automates workflows to reduce the need to switch between different security tools and tasks, while our Falcon Insight XDR module provides a unified solution that enables security teams to rapidly and efficiently identify, hunt, and eliminate threats across multiple security domains using first and third party datasets.

•Lower Total Cost of Ownership: Our cloud-native platform eliminates our customers' need for initial or ongoing purchases of hardware and does not require their personnel to configure, implement or integrate disparate point products. Additionally, our comprehensive platform reduces overall personnel costs associated with ongoing maintenance, as well as the need for software patches and upgrades for separate products.

* * *

Our research and development organizations are responsible for the design, architecture, operation and quality of our cloud native Falcon platform. In addition, the research and development organizations work closely with our customer success teams to promote customer satisfaction.

Our success is a result of our continuous drive for innovation. Our internal team of security experts, researchers, intelligence analysts, and threat hunters continuously analyzes the evolving global threat landscape to develop products that defend against today's most sophisticated and stealthy attacks and report on emerging security issues. We invest substantial resources in research and development to enhance our Falcon platform, and develop new cloud modules, features and functionality. We believe timely development of new, and enhancement of our existing products, services, and features is essential to maintaining our competitive position. We work closely with our customers and channel partners to gain valuable insight into their security management practices to assist us in designing new cloud modules and features that extend the capability of our platform. Our technical staff monitors and tests our software on a regular basis, and we also make our Falcon platform available for third-party validation. We also maintain a regular release process to update and enhance our existing solutions. In addition, we engage security

consulting firms to perform periodic vulnerability analysis of our solutions.

* * *

Our cybersecurity risk management program, which includes data privacy, product security, and information security, is designed to align with our industry's best practices.

103. With respect to risk factors, the 2024 10-K stated:

If our solutions fail or are perceived to fail to detect or prevent incidents or have or are perceived to have defects, errors, or vulnerabilities, our brand and reputation would be harmed, which would adversely affect our business and results of operations.

Real or perceived defects, errors or vulnerabilities in our Falcon platform and cloud modules, the failure of our platform to detect or prevent incidents, including advanced and newly developed attacks, misconfiguration of our solutions, or the failure of customers to take action on attacks identified by our platform could harm our reputation and adversely affect our business, financial position and results of operations.

* * *

We rely on third-party data centers, such as Amazon Web Services, and our own colocation data centers to host and operate our Falcon platform, and any disruption of or interference with our use of these facilities may negatively affect our ability to maintain the performance and reliability of our Falcon platform which could cause our business to suffer.

Our customers depend on the continuous availability of our Falcon platform. We currently host our Falcon platform and serve our customers using a mix of third-

party data centers, primarily Amazon Web Services, Inc., or AWS, and our data centers, hosted in colocation facilities. Consequently, we may be subject to service disruptions as well as failures to provide adequate support for reasons that are outside of our direct control. We have experienced and expect that in the future we may experience interruptions, delays and outages in service and availability from time to time due to a variety of factors, including infrastructure changes, human or software errors, website hosting disruptions and capacity constraints.

The following factors, many of which are beyond our control, can affect the delivery, availability, and the performance of our Falcon platform:

* * *

•errors, defects or performance problems in our software, including third-party software incorporated in our software;
•improper deployment or configuration of our solutions;
•the failure of our redundancy systems, in the event of a service disruption at one of our data centers, to provide failover to other data centers in our data center network; and
•the failure of our disaster recovery and business continuity arrangements.

The adverse effects of any service interruptions on our reputation, results of operations, and financial condition may be disproportionately heightened due to the nature of our business and the fact that our customers have a low tolerance for interruptions of any duration. Interruptions or failures in our service delivery could result in a cyberattack or other security threat to one of our customers during such periods of interruption or failure. Additionally, interruptions or failures in our service could cause customers to terminate their subscriptions with us, adversely affect our renewal rates, and harm our ability to

> attract new customers. Our business would also be harmed if our customers believe that a cloud-based SaaS-delivered endpoint security solution is unreliable. While we do not consider them to have been material, we have experienced, and may in the future experience, service interruptions and other performance problems due to a variety of factors. The occurrence of any of these factors, or if we are unable to rapidly and cost-effectively fix such errors or other problems that may be identified, could damage our reputation, negatively affect our relationship with our customers or otherwise harm our business, results of operations and financial condition.

(Emphasis in original).

March 7, 2024 Morgan Stanley Technology, Media & Telecom Conference

104. Also on March 7, 2024, Defendant Kurtz attended the Morgan Stanley Technology, Media & Telecom Conference, where he represented that it was "friction-free to deploy [CrowdStrike's product]."

105. The foregoing statements were materially false and misleading because they failed to disclose, *inter alia*, that: (1) CrowdStrike and the Individual Defendants failed to ensure that the Company had adequately developed, tested, and deployed updates to Falcon; (2) due to these failures, there was a significant risk that an update to Falcon could cause major outages for a substantial portion of CrowdStrike's customers; and (3) such outages made CrowdStrike vulnerable to substantial reputational harm and legal risk, which risks eventually materialized as a result of the CrowdStrike Outage. As a result of the foregoing, Defendants'

statements were materially false and misleading and/or lacked a reasonable basis at all relevant times.

2024 Proxy Statement

106. On May 6, 2024, CrowdStrike filed the 2024 Proxy Statement with the SEC. Defendants Kurtz, Austin, Davis, Flower, Gandhi, O'Leary, Schumacher, Sullivan, and Watzinger solicited the 2024 Proxy Statement, filed pursuant to Section 14(a) of the Exchange Act, which contained material misstatements and omissions.

107. The 2024 Proxy Statement called for shareholder approval of, *inter alia*: (1) the re-election of Defendants Austin, Gandhi, and Watzinger to the Board; (2) the ratification of the selection of PricewaterhouseCoopers LLP as CrowdStrike's independent registered public accounting firm for its fiscal year ending January 31, 2025; and (3) the approval, on an advisory basis, of the compensation of CrowdStrike's named executive officers.

108. With respect to the "Role of the Board in Risk Oversight," the 2024 Proxy Statement stated the following:

> Risk is inherent with every business, and we face a number of risks, including strategic, financial, business and operational, cybersecurity, legal and compliance, and reputational risks, in the pursuit and achievement of our strategic objectives. We have designed and implemented processes to manage risk in our operations. Management is responsible for the day-to-day oversight and management of strategic, operational, legal and

> compliance, cybersecurity, and financial risks, while our Board, as a whole and assisted by its committees, has responsibility for the oversight of our risk management framework, which is designed to identify, assess, and manage risks to which our Company is exposed, as well as foster a corporate culture of integrity. Consistent with this approach, our Board regularly reviews our strategic and operational risks in the context of discussions with management, question and answer sessions, and reports from the management team at each regular board meeting. Our Board also receives regular reports on all significant committee activities at each regular board meeting and evaluates the risks inherent in significant transactions.
>
> In addition, our Board has tasked designated standing committees with oversight of certain categories of risk management. Our Audit Committee assists our Board in fulfilling its oversight responsibilities with respect to risk assessment and risk management, including the Company's policies and practices pertaining to financial accounting, investment, tax, and cybersecurity matters, and discusses with management the Company's major financial risk exposures. Our Compensation Committee reviews and assesses risks arising from the Company's employee compensation policies and practices and whether any such risks are reasonably likely to have a material adverse effect on the Company. Our Nominating and Corporate Governance Committee monitors the effectiveness of our corporate governance guidelines and policies. Our Transaction Committee reviews and evaluates certain risks related to potential acquisitions of businesses, entities or technologies.
>
> Our Board believes its current leadership structure supports the risk oversight function of the Board.

109. Regarding the Code of Ethics, the 2024 Proxy Statement stated the following:

> Our Board has adopted Corporate Governance Guidelines that address items such as the qualifications and responsibilities of our directors and director candidates, including independence standards, and corporate governance policies and standards applicable to us in general. In addition, our Board has adopted a Code of Business Conduct and Ethics that applies to all our employees, officers and directors, including our Chief Executive Officer, Chief Financial Officer and other executive and senior financial officers. The full text of our Corporate Governance Guidelines and our Code of Business Conduct and Ethics are posted on our website at ir.crowdstrike.com. We will post amendments to our Code of Business Conduct and Ethics or any waivers of our Code of Business Conduct and Ethics for directors and executive officers on the same website or in filings under the Exchange Act.

110. Under the direction and watch of Defendants Kurtz, Austin, Davis, Flower, Gandhi, O'Leary, Schumacher, Sullivan, and Watzinger, the 2024 Proxy Statement was materially false and misleading and failed to disclose, *inter alia*, that: (1) CrowdStrike and the Individual Defendants failed to ensure that the Company had adequately developed, tested, and deployed updates to Falcon; (2) due to these failures, there was a significant risk that an update to Falcon could cause major outages for a substantial portion of CrowdStrike's customers; and (3) such outages made CrowdStrike vulnerable to substantial reputational harm and legal risk, which risks eventually materialized as a result of the CrowdStrike Outage. As a result of the foregoing, Defendants' statements were materially false and misleading and/or lacked a reasonable basis at all relevant times.

111. The 2024 Proxy Statement also failed to disclose, *inter alia*, that: (1) although the Company claimed its officers and directors adhered to the Code of Ethics, the Individual Defendants violated the Company's own internal policies; and (2) contrary to the 2024 Proxy Statement's descriptions of the Board's and its committees' risk oversight functions, the Board and its committees were not adequately exercising these functions and were (a) causing or permitting the Company to issue false and misleading statements and (b) participating in and/or facilitating the Company's participation in the testing failures as described herein.

112. As a result of Defendants Kurtz, Austin, Davis, Flower, Gandhi, O'Leary, Schumacher, Sullivan, and Watzinger causing the 2024 Proxy Statement to be false and misleading, Company shareholders voted, *inter alia*, to re-elect Defendants Austin, Gandhi, and Watzinger to the Board, thereby allowing them to continue breaching their fiduciary duties to CrowdStrike.

June 5, 2024 10-Q

113. On June 5, 2024, the Company filed a Form 10-Q with the SEC, reporting its financial and operational results for the first quarter of fiscal year 2025 ended April 30, 2024 (the "**1Q25 10-Q**"). Attached to the 1Q25 10-Q were SOX certifications made and signed by Defendants Kurtz and Podbere certifying that the 1Q25 10-Q "fully complies with the requirements of Section 13(a) or 15(d) of the [Exchange Act]" and that the "information contained in the [1Q25 10-Q] fairly

presents, in all material respects, the financial condition and results of operations of [the Company]."

114. With respect to risks affecting the Company's business, the 1Q25 10-Q stated:

> If our solutions fail or are perceived to fail to detect or prevent incidents or have or are perceived to have defects, errors, or vulnerabilities, our brand and reputation would be harmed, which would adversely affect our business and results of operations.
>
> Real or perceived defects, errors or vulnerabilities in our Falcon platform and cloud modules, the failure of our platform to detect or prevent incidents, including advanced and newly developed attacks, misconfiguration of our solutions, or the failure of customers to take action on attacks identified by our platform could harm our reputation and adversely affect our business, financial position and results of operations.
>
> * * *
>
> We rely on third-party data centers, such as Amazon Web Services, and our own colocation data centers to host and operate our Falcon platform, and any disruption of or interference with our use of these facilities may negatively affect our ability to maintain the performance and reliability of our Falcon platform which could cause our business to suffer.
>
> Our customers depend on the continuous availability of our Falcon platform. We currently host our Falcon platform and serve our customers using a mix of third-party data centers, primarily Amazon Web Services, Inc., or AWS, and our data centers, hosted in colocation facilities. Consequently, we may be subject to service disruptions as well as failures to provide adequate support for reasons that are outside of our direct control. We have

experienced, and expect that in the future we may experience interruptions, delays and outages in service and availability from time to time due to a variety of factors, including infrastructure changes, human or software errors, website hosting disruptions and capacity constraints.

The following factors, many of which are beyond our control, can affect the delivery, availability, and the performance of our Falcon platform:

•errors, defects or performance problems in our software, including third-party software incorporated in our software;
•improper deployment or configuration of our solutions;
•the failure of our redundancy systems, in the event of a service disruption at one of our data centers, to provide failover to other data centers in our data center network; and
•the failure of our disaster recovery and business continuity arrangements.

The adverse effects of any service interruptions on our reputation, results of operations, and financial condition may be disproportionately heightened due to the nature of our business and the fact that our customers have a low tolerance for interruptions of any duration. Interruptions or failures in our service delivery could result in a cyberattack or other security threat to one of our customers during such periods of interruption or failure. Additionally, interruptions or failures in our service could cause customers to terminate their subscriptions with us, adversely affect our renewal rates, and harm our ability to attract new customers. Our business would also be harmed if our customers believe that a cloud-based SaaS-delivered endpoint security solution is unreliable. While we do not consider them to have been material, we have experienced, and may in the future experience, service interruptions and other performance problems due to a variety of factors. The occurrence of any of these factors, or if we are unable

> to rapidly and cost-effectively fix such errors or other problems that may be identified, could damage our reputation, negatively affect our relationship with our customers or otherwise harm our business, results of operations and financial condition.

115. The above statements were materially false and misleading because they failed to disclose, *inter alia*, that: (1) CrowdStrike and the Individual Defendants failed to ensure that the Company had adequately developed, tested, and deployed updates to Falcon; (2) due to these failures, there was a significant risk that an update to Falcon could cause major outages for a substantial portion of CrowdStrike's customers; and (3) such outages made CrowdStrike vulnerable to substantial reputational harm and legal risk, which risks eventually materialized as a result of the CrowdStrike Outage. As a result of the foregoing, Defendants' statements were materially false and misleading and/or lacked a reasonable basis at all relevant times.

The Truth Emerges

116. The truth began to emerge on July 19, 2024, when it was publicly revealed that a flawed content update for Falcon, specifically in the program's Rapid Response Content file, caused severe worldwide technology outages for millions of devices using Microsoft Windows. The CrowdStrike Outage impacted approximately 8.5 million Windows devices, and victims of the Outage included both government entities and large corporations. Among other consequences of the

Outage, airlines were forced to ground numerous flights, and emergency 911 hotlines were inoperable. In addition, the Company warned the public that bad actors were attempting to exploit the CrowdStrike Outage as a means of hacking the Company's customers.

117. On this news, the price per share of CrowdStrike's stock fell $38.09, or 11%, from a closing price of $343.05 per share on July 18, 2024, to close at a price of $304.96 per share on July 19, 2024.

118. The truth continued to come to light on July 22, 2024, when news emerged that Congress had contacted Defendant Kurtz to testify regarding the CrowdStrike Outage. The same day, analysts such as Guggenheim and BTIG downgraded CrowdStrike's stock rating.

119. On this news, the price per share of CrowdStrike's stock fell $41.05, or 13.5%, from a closing price of $304.96 per share on July 19, 2024, to close at $263.91 on July 22, 2024.

120. On July 29, 2024, news emerged that Delta had employed renowned attorney David Boies to seek damages from CrowdStrike resulting from the CrowdStrike Outage.

121. On this news, the price per share of CrowdStrike's stock fell $25.16, or 10%, from a closing price of $258.81 on July 29, 2024, to close at $233.65 per share on July 30, 2024.

122. In the weeks following the CrowdStrike Outage, the insufficient precautions taken by CrowdStrike with regard to its updates continued to come to light. For example, *The Verge* reported that the testing CrowdStrike did on its Rapid Response Content updates did not appear to be as thorough as the testing the Company had done on other updates. Indeed, *The Verge* quoted an expert who acknowledged that "[i]f CrowdStrike had properly tested its content updates," the CrowdStrike Outage would likely not have happened. Similarly, an expert cited by *The Washington Post* represented that it was "alarming" that the Company's update was not "tested and validated" before it was implemented.

Board Minutes and Presentations Evidence Management's and the Board's Lack of Both Attention and Due Care with Respect to the Company's Core Product

123. The Outage stemmed from a faulty Rapid Response Content Update (Channel File 291), which had bypassed rigorous testing due to its classification as a "quick-deploy fix" rather than core Sensor Content. The Company's confidential Section 220 Production of Board and committee minutes, [redacted]

[redacted]

124. Defendant Kurtz should have been particularly attuned to this risk, considering his experience as McAfee's Chief Technology Officer ("**CTO**") during a significant outage in 2010.

125. Kurtz, McAfee's CTO from 2009 to 2011, was responsible for McAfee's technology strategy and customer-facing technical operations. On April 21, 2010, McAfee released a security update (DAT file version 5958) for its antivirus software, primarily targeting corporate users. The update falsely identified "svchost.exe," a critical Windows system file, as a virus ("**W32/Wecorl.a**"). Quarantining or deleting this file disrupted essential Windows processes.

126. Millions of Windows XP Service Pack 3 systems crashed globally, showing the "Blue Screen of Death" or entering continuous reboot loops. Affected organizations spanned healthcare, retail, law enforcement, and government, with significant operational disruptions.[11]

[11] *See* Sanya Jain, *Not his first rodeo: CrowdStrike CEO was also involved in another global tech disaster*, Hindustan Times (July 20, 2024)("Friday's CrowdStrike outage is the second major tech meltdown that founder and CEO George Kurtz has been involved in."), https://www.hindustantimes.com/trending/crowdstrike-ceo-george-kurtz-was-cto-of-mcafee-in-2010-global-tech-disaster-101721471586633.html.

127. Reports estimated tens of thousands to millions of affected devices, making it a major IT failure at the time.

128. McAfee retracted the update and issued a fix, but recovery required manual intervention—booting into Safe Mode, restoring the file, and applying corrected definitions. This process was time-consuming and resource-intensive.

129. The outage tarnished McAfee's reputation, contributed to its $7.7 billion acquisition by Intel in August 2010, and saw Kurtz leave in 2011 to found CrowdStrike in 2012, with the help of Defendant Davis and Warburg Pincus.

130. Gerhard Watzinger, the Company's chairman, was also a McAfee executive from 2003–2007. He served as Chief Strategy Officer and Executive Vice President, joining McAfee following its acquisition of his company, iKODE, where he had been CEO. From 2007 to 2011, he was the General Manager of the Data Protection Business Unit, overseeing key aspects of McAfee's product strategy and operations.

131. Watzinger's time at McAfee overlapped with Kurtz's tenure as CTO (2009-2011), and both worked for McAfee during the notable outage in April 2010. Like Kurtz, Watzinger ultimately left McAfee in 2011, shortly after its $7.7 billion acquisition by Intel in August 2010, and later joined CrowdStrike as chairman in April 2012.

132. Accordingly, the McAfee outage of 2010 and the CrowdStrike outage of 2024,[12] both linked to Defendant Kurtz and, to a lesser degree, Defendant Watzinger, reveal a pattern of catastrophic update failures in cybersecurity firms under Kurtz's leadership. [13]

133. [redacted] Given Falcon's deep integration into customer systems (running at the Windows kernel level), [redacted]

134. [redacted]

[12] Akash Pandey, *McAfee-caused PC meltdown and Microsoft-CrowdStrike outage have a common connection*, NewsBytes (July 20, 2024), https://www.newsbytesapp.com/news/science/defective-mcafee-once-caused-worldwide-meltdown-of-windows-xp-pcs/story.

[13] Ed Bott, *Defective McAfee update causes worldwide meltdown of XP PCs*., ZDNet (April 21, 2010), https://www.zdnet.com/article/defective-mcafee-update-causes-worldwide-meltdown-of-xp-pcs/.

[redacted]

135. [redacted]

136. [redacted]

[redacted]

137. [redacted]

138. [redacted]

139. [redacted]

[redacted]

140. [redacted]

141. [redacted]

142. Industry standards require rigorous testing, validation, and quality assurance processes prior to deploying updates of this nature. [redacted]

143. [redacted]

[redacted] A canary protocol is when the software distributor rolls out updates to a small, monitored subset of internal or opt-in systems first so that real-world feedback could catch issues missed in lab tests, like obscure driver conflicts.[14]

144. [redacted]

[14] See Sean Michael Kerner, *CrowdStrike outage explained: What caused it and what's next*, TechTarget (Oct. 28, 2024), https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next. *See also The Falcon's great Fall: The 2024 Update That Shook CrowdStrike's Legacy*, DataCouch (Sep. 3, 2024), https://datacouch.medium.com/the-falcons-great-fall-the-2024-update-that-shook-crowdstrike-s-legacy-1d55c89e1ac1 (detailing industry-specific testing protocols).
.

[redacted]

145. [redacted]

[redacted]

146. [redacted]

[redacted]

147. [redacted]

[redacted]

[redacted]

148. [redacted]

149. [redacted]

150. [redacted]

[redacted]

151. [redacted]

[redacted]

152. [redacted]

[redacted]

153. [redacted]

Pre-Outage Red Flags in the Form of Disruptions

Debian Linux Servers Crash

154. On April 19, 2024, CrowdStrike suffered a major disruption when certain Linux systems experienced "kernel panics" linked to the Falcon sensor. Specifically, the disruption occurred when a CrowdStrike update caused Debian Linux servers at a civic tech lab to become unbootable. This was reported on *Hacker News*, where a user described how an update, pushed on a Friday evening, led to simultaneous crashes across multiple production websites after a routine Debian patch. Logs pointed to the Falcon sensor as the culprit, and reinstalling it triggered immediate crashes again.

155. CrowdStrike acknowledged a "bug" a day later but took weeks to provide a full explanation, revealing the setup was not in their testing matrix. This was not a "one-off kernel panic" but a systemic failure tied to incompatibility with Debian's stable kernel (likely 6.1.0-18 or 6.1.0-20).[15]

[15] Dev Kundaliya, *CrowdStrike updates caused Linus outage in April*, THECHANNELCO (July 24, 2024), https://www.computing.co.uk/news/4338038/crowdstrike-updates-caused-linux-outages-april.

Rocky Linux 9.4 Crashes

156. On May 9, 2024, users of Rocky Linux 9.4—a community-driven, enterprise-grade Linux distribution designed as a downstream rebuild of Red Hat Enterprise Linux ("**RHEL**")—began reporting system crashes after upgrading to the latest version. These crashes manifested as kernel panics, a severe type of failure in Linux where the operating system detects a critical error and halts to prevent further damage. The issue was traced back to systems running kernel version 5.14.0-427.13.1.el9_4.x86_64, the same kernel implicated in the June 2024 Red Hat Enterprise Linux 9.4 disruption discussed below. The common factor in both cases was CrowdStrike's Falcon Sensor, a security agent that operates at the kernel level to provide endpoint protection.

157. After upgrading to Rocky Linux 9.4 (which aligned with RHEL 9.4's release cadence), systems with the Falcon Sensor installed would boot successfully but then crash with a kernel panic. The panic was linked to the Falcon Sensor's kernel module (falcon_lsm_serviceable), which uses eBPF (extended Berkeley Packet Filter) to monitor system activity. The exact trigger appeared to be an incompatibility or bug in how the sensor interacted with this specific kernel version.

158. CrowdStrike's support team confirmed the issue after users reported it through support channels and community forums. The crashes were reproducible on

systems running the affected kernel, pointing to a flaw in the Falcon Sensor's integration with Rocky Linux 9.4's updated kernel.

159. CrowdStrike suggested two primary mitigations: (i) Switch to Kernel Mode, adjusting the Falcon Sensor's configuration to operate differently within the kernel, potentially bypassing the buggy interaction (though specifics on this mode switch weren't widely detailed publicly) or; (ii) Revert to an Earlier Kernel, rolling back to a previous kernel version (*e.g.*, from an earlier Rocky Linux 9.3 or 9.2 build) where the Falcon Sensor had been stable. This was a practical, if temporary, fix while a proper solution was developed.

160. Rocky Linux 9.4, like RHEL 9.4, had shipped with kernel 5.14.0-427.13.1.el9_4.x86_64 as part of its May 2024 update cycle. This kernel introduced changes or updates that exposed a latent issue in the Falcon Sensor's eBPF implementation. Since Rocky Linux is binary-compatible with RHEL, it's unsurprising that the same kernel bug affected both distributions. The Falcon Sensor's reliance on low-level kernel hooks—designed to provide deep visibility into system behavior—made it particularly sensitive to kernel changes, and the May 2024 incident highlighted a lack of preemptive testing or compatibility validation by CrowdStrike for this specific kernel release.[16]

[16] *See* RockyLinux: *Crowdstrike freezing RockyLinus Adter 9.4 upgrade* (May 2024), https://forums.rockylinux.org/t/crowdstrike-freezing-rockylinux-after-9-4-upgrade/14041. *See also* Pradeep Viswanathan, *CrowdStrike broke Debian and Rock Linux months ag, but no one*

161. [redacted]

162. In June 2024, Red Hat reported a kernel panic tied to the Falcon sensor on Red Hat Enterprise Linux (RHEL) 9.4, observed after booting kernel version 5.14.0-427.13.1.el9_4.x86_64. This was detailed in a Red Hat advisory, attributing the crash to an eBPF program in the sensor. The panic occurred due to a bug in the Linux kernel's eBPF verifier, not directly CrowdStrike's code, though their sensor triggered it.[17]

163. Red Hat's response was to advise users to contact CrowdStrike for troubleshooting assistance and, as a temporary fix, to disable the Falcon Sensor to prevent crashes. This incident did not garner the same widespread attention as the July 19 Windows outage—likely because Linux has a smaller enterprise desktop

noticed (July 19, 2024), https://www.neowin.net/news/crowdstrike-broke-debian-and-rocky-linux-months-ago-but-no-one-noticed/ ("This was not an isolated incident. CrowdStrike users also reported similar issues after upgrading to RockyLinux 9.4, with their servers crashing due to a kernel bug. Crowdstrike support acknowledged the issue, highlighting a pattern of inadequate testing and insufficient attention to compatibility issues across different operating systems.").

[17] Simon Sharwood, *CrowdStrike's Falcon Sensor also linked to Linux kernel panics and crashes* (July 21, 2024), https://www.theregister.com/2024/07/21/crowdstrike_linux_crashes_restoration_tools/.

footprint compared to Windows, and the affected systems were fewer in number. However, it hinted at potential vulnerabilities in CrowdStrike's systems across multiple platforms, not just Windows.[18]

164. Accordingly, in May and June 2024, there were two RHEL-related events.

165. [redacted]

166. These Linux disruptions, though smaller in scale and different in mechanism from the July Windows Outage (which involved a Rapid Response Content update), highlighted vulnerabilities in the Falcon Sensor's kernel-level operations across platforms [redacted]

167. [redacted] especially since the sensor operates with deep system access—a known risk area. [redacted]

[18] *See id.*

[redacted]

a. **Regression Testing:** Regression Testing is a well-established practice in software development, particularly for companies delivering updates to mission-critical systems. It involves re-running functional and non-functional tests to ensure that new changes—whether code, configuration, or content—do not break existing functionality. For a cybersecurity firm like CrowdStrike, whose platforms operate at the kernel level of operating systems and protects against threats in real time, regression testing would be considered standard practice to prevent unintended disruptions, such as the global Outage caused by a faulty update in July 2024. Skipping regression testing, especially for updates affecting core functionality or system stability, deviates from industry norms, as it risks introducing defects that could have catastrophic downstream effects.[19]

[19] See Phil Richard, *The Importance of Regression Testing: What IT Leaders Can Lean from CrowdStrike*, L2L.com (Jul 25, 2025), https://www.l2l.com/blog/regression-testing.

b. **Sandbox Environment Testing:** Sandbox Environment Testing involves running software in an isolated, controlled setting that mimics real-world conditions to evaluate its behavior without impacting production systems. In the cybersecurity industry, where updates must detect new threats without compromising system integrity, sandbox testing is a standard tool. CrowdStrike itself uses sandboxing as part of its threat analysis process for analyzing malicious payloads.[20] Extending this to test updates in a sandbox environment before deployment aligns with best practices, ensuring compatibility and stability across diverse configurations (*e.g.*, different OS versions or hardware). While not every update might require exhaustive sandbox testing, it would be standard for significant or high-risk changes to undergo such validation.[21]

c. **Canary Deployment:** Canary Deployment is a deployment strategy where updates are rolled out gradually to a small subset of users or

[20] Bart Lenarts-Bergmans, *What is Cybersecurity Sandboxing?* (Sept. 11, 2023), https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/cybersecurity-sandboxing/.

[21] *See* https://www.lambdatest.com/software-testing-questions/what-is-sandbox ("The primary purpose of a sandbox is to provide a testing environment that mimics the live (production) environment. However, it is excluded from other organization assets like the servers used to run websites, applications, and databases that store user details. Using this approach, testing issues are limited to the sandbox and won't jeopardize other systems and resources.").

systems before a full release, allowing early detection of issues with minimal impact.[22] This practice is increasingly standard in modern software development, especially for cloud-native or widely distributed systems like CrowdStrike's Falcon platform. It mitigates risk by providing real-world feedback without exposing the entire user base to potential failures.[23] Historically, CrowdStrike did not use canary deployments for certain "Rapid Response Content" updates, as revealed after the July 2024 incident, where a lack of staged rollout contributed to widespread disruption. However, by 2025, canary deployment is considered a standard practice for critical software providers, and CrowdStrike has since committed to adopting it, suggesting it was not previously routine for all update types but is now recognized, as necessary.[24]

d. **Security Validation:** Security Validation ensures that updates do not introduce vulnerabilities or weaken existing protections. For a

[22] Nnenna Ndukwe, *Canary releases with feature flags: how to*, Unleash (May 23, 2024), https://www.getunleash.io/blog/canary-deployment-what-is-it.

[23] Rahul Awati & Peter Loshin, *Definition: Canary Testing*, Techtarget.com (https://www.techtarget.com/whatis/definition/canary-canary-testing, last visited March 31, 2025, 1:15 AM.

[24] *Canary deployments: Pros, cons, and 5 critical best practices*,

Octopus Deploy (https://octopus.com/devops/software-deployments/canary-deployment/, last visited March 31, 2025, 1:25 AM.

cybersecurity company like CrowdStrike, this is not just standard—it is essential.[25] Validation typically includes testing for secure coding practices, ensuring no exploitable flaws are introduced, and verifying that the update maintains or enhances threat detection capabilities. This can involve automated checks, manual audits, or adversarial testing (*e.g.*, red teaming).[26] Given CrowdStrike's role in protecting against sophisticated threats, security validation would be a baseline expectation for all updates, whether code-based or content-driven, to maintain trust and efficacy.[27]

[25] Amanda McCarvill, *An Introduction to the Importance of Input Validation in Preventing Security Vulnerabilities*, Bright (August 11, 2023) https://brightsec.com/blog/an-introduction-to-the-importance-of-input-validation-in-preventing-security-vulnerabilities/ ("Input validation also plays a crucial role in maintaining the accuracy and integrity of data. By ensuring that only valid and trustworthy information is accepted, it prevents errors or inconsistencies that could compromise the quality of data stored or processed. For example, proper input validation would check if a month entered fell between 1 and 12. Without proper validation, erroneous data could be entered or crash the application. In essence, strong input validation is a frontline defense, fortifying applications against unauthorized access, attacks, and maintaining the reliability of the information they handle.").

[26] Paul Kirvan, *What is red teaming?* TechTarget https://www.techtarget.com/whatis/definition/red-teaming, last visited March 30, 2025.

[27] *What Is Secure Software Development Lifecycle (Secure SDLC)?*.Paloalto Networks, https://www.paloaltonetworks.com/cyberpedia/what-is-secure-software-development-lifecycle, last visited March 31, 2025, 3:00 PM.

DAMAGES TO CROWDSTRIKE

168. As a direct and proximate result of the Individual Defendants' conduct, CrowdStrike has lost and expended, and will continue to lose and expend, many millions of dollars. Such expenditures include, but are not limited to:

a. legal fees, costs, and any payments for resolution of or to satisfy a judgment associated with the Securities Class Action or the Consumer Class Actions, and amounts paid to outside lawyers, accountants, and investigators in connection therewith;

b. legal fees, costs, and any payments for resolution of or to satisfy judgements associated with any other lawsuits filed against the Company or the Individual Defendants based on the Outage, including the Delta lawsuit, which indicates that Delta suffered more than $500 million in out-of-pocket losses as a result of the Outage;

c. the cost of implementing measures to remediate fallout from the Outage;

d. costs incurred in any internal investigations pertaining to violations of law, costs incurred in defending any investigations or legal actions taken against the Company due to its violations of law, and payments of any fines or settlement amounts associated with the Company's violations;

e. unjust compensation, benefits, and other payments provided to the Individual Defendants who breached their fiduciary duties to the Company; and

f. any other losses stemming from the Outage.

169. As a direct and proximate result of the Individual Defendants' conduct, CrowdStrike has also suffered and will continue to suffer a loss of reputation and goodwill, and a "liar's discount" that will plague the Company's stock price in the future due to the Company's and their misrepresentations.

DERIVATIVE & DEMAND FUTILITY ALLEGATIONS

170. Plaintiff brings this action derivatively, in the right and for the benefit of CrowdStrike, to redress injuries suffered, and to be suffered, as a result of the Individual Defendants' breaches of their fiduciary duties as directors and/or officers of CrowdStrike, unjust enrichment, and violations of the Exchange Act.

171. CrowdStrike is named solely as a nominal party in this action. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have.

172. Plaintiff is, and has been at all relevant times, a shareholder of CrowdStrike.

173. Plaintiff will adequately and fairly represent the interests of CrowdStrike in enforcing and prosecuting its rights, and, to that end, has retained

competent counsel, experienced in derivative litigation, to enforce and prosecute this action.

174. Plaintiff incorporates by reference and re-alleges each and every allegation stated above as if fully set forth herein.

175. A pre-suit demand on the Board is futile and, therefore, excused. At the time of the commencement of this action, the Board consisted of the following nine individuals: Defendants Kurtz, Austin, Davis, Flower, Gandhi, O'Leary, Schumacher, Sullivan, and Watzinger (the "**Director Defendants**"). Plaintiff needs only to allege demand futility as to five of these nine Director Defendants.

176. Demand is excused as to all of the Director Defendants because each faces, individually and collectively, a substantial likelihood of liability as a result of the schemes they engaged in, knowingly or recklessly, to cause the Company to fail to adequately develop, test, and deploy updates to Falcon, and to make and/or cause the Company to make false and misleading statements and omissions of material facts. This renders the Director Defendants unable to impartially investigate the charges and decide whether to pursue action against themselves and the other perpetrators of the schemes.

177. In complete abdication of their fiduciary duties, the Director Defendants either knowingly or recklessly participated in: (i) causing the Company to fail to adequately develop, test, and deploy updates to Falcon; and (ii) making

and/or causing the Company to make the materially false and misleading statements alleged herein. The fraudulent schemes were intended to make the Company appear more profitable and attractive to investors. Moreover, the Director Defendants caused the Company to fail to maintain internal controls. As a result of the foregoing, the Director Defendants breached their fiduciary duties, face a substantial likelihood of liability, are not disinterested, and demand upon them is futile, and thus excused.

Additional Reasons that Demand is Futile

178. Defendant Kurtz has served as CrowdStrike's President, CEO, and a director since November 2011. As such, the Company provides Defendant Kurtz with his principal occupation, for which he receives lucrative compensation. Thus, as the Company admits, Defendant Kurtz is a non-independent director. As CrowdStrike's CEO and as one of its trusted directors, Defendant Kurtz was ultimately responsible for all of the false and misleading statements and omissions that were made by or on behalf of the Company during the Relevant Period, including those which he personally signed and for which he made SOX certifications. As a trusted Company director, Defendant Kurtz conducted little, if any, oversight of the schemes to cause the Company to fail to adequately develop, test, and deploy updates to Falcon and to make false and misleading statements, consciously disregarded his duties to monitor internal controls over reporting and

engagement in the schemes, and consciously disregarded his duties to protect corporate assets.

179. In addition, Defendant Kurtz signed the 2024 10-K, which contained false and misleading statements, and solicited the 2024 Proxy Statement, which contained false and misleading statements and resulted in, *inter alia*, the re-election of Defendants Austin, Gandhi, and Watzinger to the Board, thereby allowing them to continue breaching their fiduciary duties to CrowdStrike.

180. Further, Defendant Kurtz's insider sales, made with knowledge of material nonpublic information before the material misstatements and omissions were exposed, demonstrate his motive to facilitate and participate in the scheme. Kurtz sold over 78,080 shares for over $25 million on March 21, 2024 – just weeks before the April incident. He sold 56,279 shares for over $17 million just six days before the May incident. Finally, he sold 55,587 shares on June 21, for almost $21 million—less than 30 days before the Outage and just weeks after the June 4, Red Hat incident.

181. Moreover, Defendant Kurtz is named as a defendant in the Securities Class Action. For these reasons, Defendant Kurtz breached his fiduciary duties, faces a substantial likelihood of liability, is not independent or disinterested, and thus demand upon him is futile and, therefore, excused.

182. Defendant Austin has served as a Company director since September 2018. She also serves as Chair of the Audit Committee. Defendant Austin has received and continues to receive lucrative compensation for her role as a director, as described above. As a trusted Company director, she conducted little, if any, oversight of the schemes to cause the Company to fail to adequately develop, test, and deploy updates to Falcon and to make false and misleading statements, consciously disregarded her duties to monitor internal controls over reporting and engagement in the schemes, and consciously disregarded her duties to protect corporate assets.

183. In addition, Defendant Austin signed the 2024 10-K, which contained false and misleading statements, and solicited the 2024 Proxy Statement, which contained false and misleading statements and resulted in, *inter alia*, the re-election of herself and Defendants Gandhi and Watzinger to the Board, thereby allowing them to continue breaching their fiduciary duties to CrowdStrike.

184. Further, Defendant Austin's insider sales, made with knowledge of material nonpublic information before the material misstatements and omissions were exposed, demonstrate her motive to facilitate and participate in the scheme. Defendant Austin sold 15,000 shares for over $5 million between June 27 and 28, 2024—just a few weeks after the April, May, and June incidents, and just weeks before the Outage. For these reasons, Defendant Austin breached her fiduciary

duties, faces a substantial likelihood of liability, is not independent or disinterested, and thus demand upon her is futile and, therefore, excused.

185. Defendant Davis has served as a Company director since July 2013. He also serves as a member of the Compensation Committee. Defendant Davis has received and continues to receive lucrative compensation for his role as a director, as described above. As a trusted Company director, he conducted little, if any, oversight of the schemes to cause the Company to fail to adequately develop, test, and deploy updates to Falcon and to make false and misleading statements, consciously disregarded his duties to monitor internal controls over reporting and engagement in the schemes, and consciously disregarded his duties to protect corporate assets.

186. In addition, Defendant Davis signed the 2024 10-K, which contained false and misleading statements, and solicited the 2024 Proxy Statement, which contained false and misleading statements and resulted in, *inter alia*, the re-election of Defendants Austin, Gandhi and Watzinger to the Board, thereby allowing them to continue breaching their fiduciary duties to CrowdStrike.

187. Moreover, Defendant Davis, a Managing Director at Warburg Pincus, joined the CrowdStrike board due to the firm's early investment in the Company. Warburg Pincus provided $25 million in initial funding in 2011, when Kurtz was an entrepreneur-in-residence at the firm after leaving McAfee. Warburg Pincus made

~$1.91 billion in unrealized profit at the $34 IPO price, or ~$3.32 billion at the $58 close, assuming a $90 million investment. Davis has been with Warburg Pincus since 1994.

188. Accordingly, Davis is not independent of Kurtz because they enjoy an investor-founder dynamic built on mutual professional respect. Kurtz's time at Warburg Pincus and Davis's ongoing Board presence (representing a once key stakeholder) imply regular interaction over 13 years. This longevity fosters a personal rapport and renders Davis unable to pursue litigation against Kurtz. For these reasons, Defendant Davis breached his fiduciary duties, faces a substantial likelihood of liability, is not independent or disinterested, and thus demand upon him is futile and, therefore, excused.

189. Defendant Flower has served as a Company director since January 2023. Defendant Flower has received and continues to receive lucrative compensation for her role as a director, as described above. As a trusted Company director, she conducted little, if any, oversight of the schemes to cause the Company to fail to adequately develop, test, and deploy updates to Falcon and to make false and misleading statements, consciously disregarded her duties to monitor internal controls over reporting and engagement in the schemes, and consciously disregarded her duties to protect corporate assets.

190. In addition, Defendant Flower signed the 2024 10-K, which contained false and misleading statements, and solicited the 2024 Proxy Statement, which contained false and misleading statements and resulted in, *inter alia*, the re-election of Defendants Austin, Gandhi and Watzinger to the Board, thereby allowing them to continue breaching their fiduciary duties to CrowdStrike. For these reasons, Defendant Flower breached her fiduciary duties, faces a substantial likelihood of liability, is not independent or disinterested, and thus demand upon her is futile and, therefore, excused.

191. Defendant Gandhi has served as a Company director since August 2013. He also serves as Chair of the Compensation Committee and as a member of the Transaction Committee. Defendant Gandhi has received and continues to receive lucrative compensation for his role as a director, as described above. As a trusted Company director, he conducted little, if any, oversight of the schemes to cause the Company to fail to adequately develop, test, and deploy updates to Falcon and to make false and misleading statements, consciously disregarded his duties to monitor internal controls over reporting and engagement in the schemes, and consciously disregarded his duties to protect corporate assets. In addition, Defendant Gandhi signed the 2024 10-K, which contained false and misleading statements, and solicited the 2024 Proxy Statement, which contained false and misleading statements and resulted in, *inter alia*, the re-election of himself and Defendants Austin and

Watzinger to the Board, thereby allowing them to continue breaching their fiduciary duties to CrowdStrike.

192. Moreover Gandhi, a partner at Accel, joined the CrowdStrike Board following Accel's investment in the Company's Series B funding round in 2013. Accel invested $30 million in this round, announced on July 23, 2013, bringing CrowdStrike's total funding to $56 million at that point (including the $25 million from Warburg Pincus and an additional $1 million from other sources). This was CrowdStrike's second major funding event, following its Series A.

193. The Series B funds were used to accelerate product development, expand sales and marketing efforts, and grow CrowdStrike's customer base. By 2013, CrowdStrike had already launched its Falcon endpoint protection platform (in stealth mode since 2011, publicly in 2013), and Accel's investment helped scale its go-to-market strategy.

194. Gandhi, who is known for backing tech companies like Dropbox and Venafi, spearheaded the Accel investment and joined CrowdStrike's board of directors as part of the deal, providing strategic guidance alongside Warburg's Cary Davis.

195. Accel's $30 million infusion was critical in transitioning CrowdStrike from a startup with a promising product to a competitive enterprise player. It bridged the gap between the foundational Series A (product creation) and later rounds that

fueled global expansion. Through Gandhi's Board seat, Accel contributed industry expertise and networks, helping refine CrowdStrike's business model. Gandhi's experience with scaling tech firms likely influenced decisions on infrastructure, hiring, and market positioning.

196. In 2015, Accel participated in a $100 million round led by Google Capital (now CapitalG), valuing CrowdStrike at over $1 billion and cementing its "unicorn" status. This round, announced on July 13, 2015, included Warburg Pincus and new investors like Rackspace.

197. Accel remained involved through Series D ($200 million, June 2018, led by General Atlantic) and Series E ($200 million, June 2019, also led by General Atlantic), though its leadership role diminished as new investors took the helm. By the time of CrowdStrike's IPO in June 2019 (raising $612 million at a $6.6 billion valuation), Accel's early investment paid off significantly. It is estimated that Accel made an estimated $1.25 billion in unrealized profit at the IPO price of $34, and up to $2.2 billion based on the first-day close of $58, assuming an $80 million investment. Given this, it is highly unlikely that Gandhi would take any action against Kurtz.

198. Moreover, Gandhi sold 45,000 shares for over $13 million prior to the Outage and other incidents. For these reasons, Defendant Gandhi breached his

fiduciary duties, faces a substantial likelihood of liability, is not independent or disinterested, and thus demand upon him is futile and, therefore, excused.

199. Defendant O'Leary has served as a Company director since December 2011. He also serves as Chair of the Nominating and Corporate Governance Committee. Defendant O'Leary has received and continues to receive lucrative compensation for his role as a director, as described above. As a trusted Company director, he conducted little, if any, oversight of the schemes to cause the Company to fail to adequately develop, test, and deploy updates to Falcon and to make false and misleading statements, consciously disregarded his duties to monitor internal controls over reporting and engagement in the schemes, and consciously disregarded his duties to protect corporate assets.

200. In addition, Defendant O'Leary signed the 2024 10-K, which contained false and misleading statements, and solicited the 2024 Proxy Statement, which contained false and misleading statements and resulted in, *inter alia*, the re-election of Defendants Austin, Gandhi and Watzinger to the Board, thereby allowing them to continue breaching their fiduciary duties to CrowdStrike. Further, Defendant O'Leary's insider sales, made with knowledge of material nonpublic information before the material misstatements and omissions were exposed, demonstrate his motive in facilitating and participating in the schemes. For these reasons, Defendant O'Leary breached his fiduciary duties, faces a substantial likelihood of liability, is

not independent or disinterested, and thus demand upon him is futile and, therefore, excused.

201. Defendant Schumacher has served as a Company director since November 2020. She also serves as a member of the Nominating and Corporate Governance Committee. Defendant Schumacher has received and continues to receive lucrative compensation for her role as a director, as described above. As a trusted Company director, she conducted little, if any, oversight of the schemes to cause the Company to fail to adequately develop, test, and deploy updates to Falcon and to make false and misleading statements, consciously disregarded her duties to monitor internal controls over reporting and engagement in the schemes, and consciously disregarded her duties to protect corporate assets.

202. In addition, Defendant Schumacher signed the 2024 10-K, which contained false and misleading statements, and solicited the 2024 Proxy Statement, which contained false and misleading statements and resulted in, *inter alia*, the re-election of Defendants Austin, Gandhi and Watzinger to the Board, thereby allowing them to continue breaching their fiduciary duties to CrowdStrike. For these reasons, Defendant Schumacher breached her fiduciary duties, faces a substantial likelihood of liability, is not independent or disinterested, and thus demand upon her is futile and, therefore, excused.

203. Defendant Sullivan has served as a Company director since December 2017. He also serves as a member of the Audit Committee. Defendant Sullivan has received and continues to receive lucrative compensation for his role as a director, as described above. As a trusted Company director, he conducted little, if any, oversight of the schemes to cause the Company to fail to adequately develop, test, and deploy updates to Falcon and to make false and misleading statements, consciously disregarded his duties to monitor internal controls over reporting and engagement in the schemes, and consciously disregarded his duties to protect corporate assets. In addition, Defendant Sullivan signed the 2024 10-K, which contained false and misleading statements, and solicited the 2024 Proxy Statement, which contained false and misleading statements and resulted in, *inter alia*, the re-election of Defendants Austin, Gandhi and Watzinger to the Board, thereby allowing them to continue breaching their fiduciary duties to CrowdStrike. For these reasons, Defendant Sullivan breached his fiduciary duties, faces a substantial likelihood of liability, is not independent or disinterested, and thus demand upon him is futile and, therefore, excused.

204. Defendant Watzinger has served as a Company director since April 2012. He also serves as a member of the Audit Committee, Nominating and Corporate Governance Committee, and Transaction Committee. Defendant Watzinger has received and continues to receive lucrative compensation for his role

as a director, as described above. As a trusted Company director, he conducted little, if any, oversight of the schemes to cause the Company to fail to adequately develop, test, and deploy updates to Falcon and to make false and misleading statements, consciously disregarded his duties to monitor internal controls over reporting and engagement in the schemes, and consciously disregarded his duties to protect corporate assets.

205. In addition, Defendant Watzinger signed the 2024 10-K, which contained false and misleading statements, and solicited the 2024 Proxy Statement, which contained false and misleading statements and resulted in, *inter alia*, the re-election of himself and Defendants Austin and Gandhi to the Board, thereby allowing them to continue breaching their fiduciary duties to CrowdStrike. For these reasons, Defendant Watzinger breached his fiduciary duties, faces a substantial likelihood of liability, is not independent or disinterested, and thus demand upon him is futile and, therefore, excused.

206. Defendants Austin, Sullivan, and Watzinger served as members of the Audit Committee at all relevant times. As such, they were responsible for the effectiveness of the Company's internal controls, the truth and accuracy of the Company's financial statements, and the Company's compliance with applicable laws and regulations. During the Relevant Period, they violated the Audit Committee Charter by engaging in or permitting the Company to engage in the dissemination of

materially false and misleading statements to the public and to facilitate the Individual Defendants' violations of law, including breaches of fiduciary duty and violations of the Exchange Act; failed to adequately exercise their risk management and risk assessment functions; and failed to ensure adequate Board oversight of the Company's internal control over financial reporting, disclosure controls and procedures, and Code of Ethics. Thus, the Audit Committee Defendants breached their fiduciary duties, are not independent or disinterested, and thus demand is excused as to them.

207. In violation of the Code of Ethics, the Director Defendants engaged in or permitted the schemes to cause the Company to fail to adequately develop, test, and deploy updates to Falcon, to issue materially false and misleading statements to the investing public, and to facilitate and disguise the Individual Defendants' violations of law, including breaches of fiduciary duty, unjust enrichment, abuse of control, gross mismanagement, waste of corporate assets, and violations of the Exchange Act. In addition, the Director Defendants violated the Code of Ethics by failing to act with integrity, failing to avoid conflicts of interest, failing to prevent the Company from participating in the misconduct described herein, failing to ensure the Company's disclosures were accurate, failing to ensure the Company complied with applicable laws, rules, and regulations, and failing to promptly report known violations of the Code of Ethics and the law. Thus, the Director Defendants breached

the Company's own Code of Ethics, are not disinterested, and demand is excused as to them.

208. CrowdStrike has been and will continue to be exposed to significant losses due to the wrongdoing complained of herein, yet the Director Defendants have not filed any lawsuits against the Individual Defendants or any others who were responsible for that wrongful conduct to attempt to recover for CrowdStrike any part of the damages CrowdStrike suffered and will continue to suffer thereby. Thus, any demand upon the Director Defendants would be futile.

209. The Individual Defendants' conduct described herein and summarized above could not have been the product of legitimate business judgment as it was based on bad faith and intentional, reckless, or disloyal misconduct. Thus, none of the Director Defendants can claim exculpation from their violations of duty pursuant to the Company's charter (to the extent such a provision exists). As a majority of the Director Defendants face a substantial likelihood of liability, they are self-interested in the transactions challenged herein and are not capable of exercising independent and disinterested judgment about whether to pursue this action on behalf of the shareholders of the Company. Accordingly, demand is excused as being futile.

210. The acts complained of herein constitute violations of fiduciary duties owed by CrowdStrike's officers and directors, and these acts are incapable of ratification.

211. The Director Defendants may also be protected against personal liability for their acts of mismanagement and breaches of fiduciary duty alleged herein by directors' and officers' liability insurance if they caused the Company to purchase it for their protection with corporate funds, *i.e.*, monies belonging to the stockholders of CrowdStrike. If there is a directors' and officers' liability insurance policy covering the Director Defendants, it may contain provisions that eliminate coverage for any action brought directly by the Company against the Director Defendants, known as, *inter alia*, the "insured-versus-insured exclusion." As a result, if the Director Defendants were to sue themselves or certain of the officers of CrowdStrike, there would be no directors' and officers' insurance protection. Accordingly, the Director Defendants cannot be expected to bring such a suit. On the other hand, if the suit is brought derivatively, as this action is brought, such insurance coverage, if such an insurance policy exists, will provide a basis for the Company to effectuate a recovery. Thus, demand on the Director Defendants is futile and, therefore, excused.

212. If there is no directors' and officers' liability insurance, then the Director Defendants will not cause CrowdStrike to sue the Individual Defendants named herein, because, if they did, they would face a large uninsured individual liability. Accordingly, demand is futile in that event, as well.

213. Thus, for all of the reasons set forth above, all of the Director Defendants, and, if not all of them, at least five of the Director Defendants, cannot consider a demand with disinterestedness and independence. Consequently, a demand upon the Board is excused as futile.

FIRST CLAIM

Against the Individual Defendants

for Violations of Section 14(a) of the Exchange Act

214. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above, as though fully set forth herein.

215. Section 14(a) of the Exchange Act, 15 U.S.C. § 78n(a)(1), provides that "[i]t shall be unlawful for any person, by use of the mails or by any means or instrumentality of interstate commerce or of any facility of a national securities exchange or otherwise, in contravention of such rules and regulations as the [SEC] may prescribe as necessary or appropriate in the public interest or for the protection of investors, to solicit or to permit the use of his name to solicit any proxy or consent or authorization in respect of any security (other than an exempted security) registered pursuant to section 12 of this title [15 U.S.C. § 78l]."

216. Rule 14a-9, promulgated pursuant to Section 14(a) of the Exchange Act, provides that no proxy statement shall contain "any statement which, at the time and in the light of the circumstances under which it is made, is false or misleading

with respect to any material fact, or which omits to state any material fact necessary in order to make the statements therein not false or misleading." 17 C.F.R. § 240.14a-9.

217. Under the direction and watch of Defendants Kurtz, Austin, Davis, Flower, Gandhi, O'Leary, Schumacher, Sullivan, and Watzinger, the 2024 Proxy Statement failed to disclose, *inter alia*, that: (1) CrowdStrike and the Individual Defendants failed to ensure that the Company had adequately developed, tested, and deployed updates to Falcon; (2) due to these failures, there was a significant risk that an update to Falcon could cause major outages for a substantial portion of CrowdStrike's customers; and (3) such outages made CrowdStrike vulnerable to substantial reputational harm and legal risk, which risks eventually materialized as a result of the CrowdStrike Outage. As a result of the foregoing, Defendants' statements were materially false and misleading and/or lacked a reasonable basis at all relevant times.

218. The 2024 Proxy Statement also failed to disclose, inter alia, that: (1) although the Company claimed its officers and directors adhered to the Code of Ethics, the Individual Defendants violated these policies either without waivers or without such waivers being disclosed; and (2) contrary to the 2024 Proxy Statement's descriptions of the Board's and its committees' risk oversight functions, the Board and its committees were not adequately exercising these functions and

were (a) causing or permitting the Company to issue false and misleading statements and (b) participating in and/or facilitating the Company's participation in the failure to adequately develop, test, and deploy updates to Falcon.

219. In the exercise of reasonable care, the Individual Defendants should have known that by misrepresenting or failing to disclose the foregoing material facts, the statements contained in the 2024 Proxy Statement were materially false and misleading. The misrepresentations and omissions were material to Plaintiff in voting on the matters set forth for shareholder determination in the 2024 Proxy Statement, including, but not limited to, the election of the Company's directors.

220. As a result of the material misstatements and omissions contained in the 2024 Proxy Statement, Company shareholders voted, inter alia, to: (1) re-elect Defendants Austin, Gandhi, and Watzinger to the Board, thereby allowing them to continue breaching their fiduciary duties to CrowdStrike; and (2) approve the selection of PricewaterhouseCoopers LLP as CrowdStrike's independent registered public accounting firm for its fiscal year ending January 31, 2025.

221. The Company was damaged as a result of the Individual Defendants' material misrepresentations and omissions in the 2024 Proxy Statement.

222. Plaintiff, on behalf of CrowdStrike, has no adequate remedy at law.

SECOND CLAIM

Against the Individual Defendants

for Breach of Fiduciary Duties

223. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above, as though fully set forth herein.

224. Each Individual Defendant owed to the Company the duty to exercise candor, good faith, and loyalty in the management and administration of CrowdStrike's business and affairs.

225. Each of the Individual Defendants violated and breached his or her fiduciary duties of candor, good faith, loyalty, reasonable inquiry, oversight, and supervision.

226. The Individual Defendants' conduct set forth herein was due to their intentional or reckless breach of fiduciary duties they owed to the Company, as alleged herein. The Individual Defendants intentionally or recklessly breached or disregarded their fiduciary duties to protect the rights and interests of CrowdStrike.

227. Moreover, the Individual Defendants breached their fiduciary duties by personally making and/or causing the Company to make a series of materially false and misleading statements about CrowdStrike's business, operations, and prospects. Specifically, the Individual Defendants willfully or recklessly made and/or caused the Company to make false and misleading statements to the investing public that

failed to disclose, *inter alia*, that: (1) CrowdStrike and the Individual Defendants failed to ensure that the Company had adequately developed, tested, and deployed updates to Falcon; (2) due to these failures, there was a significant risk that an update to Falcon could cause major outages for a substantial portion of CrowdStrike's customers; and (3) such outages made CrowdStrike vulnerable to substantial reputational harm and legal risk, which risks eventually materialized as a result of the CrowdStrike Outage. As a result of the foregoing, Defendants' statements were materially false and misleading and/or lacked a reasonable basis at all relevant times.

228. In breach of their fiduciary duties, the Individual Defendants caused or permitted the Company's failure to adequately develop, test, and deploy updates to Falcon, resulting in the Outage.

229. In further breach of their fiduciary duties, the Individual Defendants failed to correct and/or caused the Company to fail to correct the false and/or misleading statements and/or omissions of material fact, which renders them personally liable to the Company for breaching their fiduciary duties.

230. Also in breach of their fiduciary duties, the Individual Defendants failed to maintain internal controls.

231. In yet further breach of their fiduciary duties, during the Relevant Period, five of the Individual Defendants engaged in lucrative insider sales, netting proceeds of over $195.5 million.

232. The Individual Defendants had actual or constructive knowledge that they had caused the Company to improperly engage in the fraudulent schemes set forth herein, including the failure to adequately develop, test, and deploy updates to Falcon, and to fail to maintain internal controls. The Individual Defendants had actual knowledge that the Company was engaging in the fraudulent schemes set forth herein, and that internal controls were not adequately maintained, or acted with reckless disregard for the truth, in that they caused the Company to improperly engage in the fraudulent schemes and to fail to maintain adequate internal controls, even though such facts were available to them. Such improper conduct was committed knowingly or recklessly and for the purpose and effect of artificially inflating the price of CrowdStrike's securities. The Individual Defendants, in good faith, should have taken appropriate action to correct the schemes alleged herein and to prevent it from continuing to occur.

233. These actions were not a good-faith exercise of prudent business judgment to protect and promote the Company's corporate interests.

234. As a direct and proximate result of the Individual Defendants' breaches of their fiduciary obligations, CrowdStrike has sustained and continues to sustain significant damages. As a result of the misconduct alleged herein, the Individual Defendants are liable to the Company.

235. Plaintiff, on behalf of CrowdStrike, has no adequate remedy at law.

THIRD CLAIM

Against the Individual Defendants

for Unjust Enrichment

236. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above, as though fully set forth herein.

237. By their wrongful acts, violations of law, and false and misleading statements and omissions of material fact that they made and/or caused to be made, the Individual Defendants were unjustly enriched at the expense of, and to the detriment of, CrowdStrike.

238. The Individual Defendants either benefitted financially from the improper conduct, received bonuses, stock options, or similar compensation from CrowdStrike that was tied to the performance or artificially inflated valuation of CrowdStrike, or received compensation or other payments that were unjust in light of the Individual Defendants' bad-faith conduct. This includes lavish compensation, benefits, and other payments provided to the Individual Defendants who breached their fiduciary duties to the Company.

239. Plaintiff, as a shareholder and representative of CrowdStrike, seeks restitution from the Individual Defendants and seeks an order from this Court disgorging all profits, including from insider transactions, benefits, and other compensation, including any performance-based or valuation-based compensation,

obtained by the Individual Defendants due to their wrongful conduct and breach of their fiduciary and contractual duties.

240. Plaintiff, on behalf of CrowdStrike, has no adequate remedy at law.

FOURTH CLAIM

Against Defendant Kurtz and Defendant Podbere

for Contribution under Sections 10(b) and 21D of the Exchange Act

241. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above, as though fully set forth herein.

242. CrowdStrike and Defendants Kurtz and Podbere are named as defendants in the Securities Class Action, which asserts claims under the federal securities laws for violations of Sections 10(b) and 20(a) of the Exchange Act, and SEC Rule 10b-5 promulgated thereunder. If and when the Company is found liable in the Securities Class Action for these violations of the federal securities laws, the Company's liability will be, in whole or in part, due to Defendant Kurtz's and Defendant Podbere's willful and/or reckless violations of their obligations as officers of CrowdStrike.

243. Defendants Kurtz and Podbere, because of their positions of control and authority as officers of CrowdStrike, were able to and did, directly and/or indirectly, exercise control over the business and corporate affairs of CrowdStrike, including the wrongful acts complained of herein and in the Securities Class Action.

244. Accordingly, Defendants Kurtz and Podbere are liable under 15 U.S.C § 78j(b), which creates a private right of action for contribution, and Section 21D of the Exchange Act, 15 U.S.C. § 78u-4(f), which governs the application of a private right of action for contribution arising out of violations of the Exchange Act

245. As such, CrowdStrike is entitled to receive all appropriate contribution or indemnification from Defendants Kurtz and Podbere.

REQUEST FOR RELIEF

FOR THESE REASONS, Plaintiff demands judgment in the Company's favor against all Individual Defendants as follows:

(a) Declaring that Plaintiff may maintain this action on behalf of CrowdStrike and that Plaintiff is an adequate representative of the Company;

(b) Declaring that the Individual Defendants have breached and/or aided and abetted the breach of their fiduciary duties to CrowdStrike;

(c) Determining and awarding to CrowdStrike the damages sustained by it as a result of the violations set forth above from each of the Individual Defendants, jointly and severally, together with pre-judgment and post-judgment interest thereon;

(d) Directing CrowdStrike and the Individual Defendants to take all necessary actions to reform and improve CrowdStrike's corporate governance and internal procedures to comply with applicable laws and

to protect CrowdStrike and its shareholders from a repeat of the damaging events described herein, including, but not limited to, putting forward for shareholder vote the following resolutions for amendments to the Company's Bylaws or Articles of Incorporation and taking the following actions as may be necessary to ensure proper corporate governance policies:

i. a proposal to strengthen the Board's supervision of operations and develop and implement procedures for greater shareholder input into the policies and guidelines of the Board;

ii. a provision to permit the shareholders of CrowdStrike to nominate at least five candidates for election to the Board; and

(e) a proposal to ensure the establishment of effective oversight of compliance with applicable laws, rules, and regulations.

(f) Awarding CrowdStrike restitution from the Individual Defendants, and each of them;

(g) Awarding Plaintiff the costs and disbursements of this action, including reasonable attorneys' and experts' fees, costs, and expenses; and

(h) Granting such other and further relief as the Court may deem just and proper.

JURY DEMAND

Plaintiff hereby demands a trial by jury.

Dated: April 9, 2025

BIELLI & KLAUDER, LLC

/s Ryan M. Ernst
Ryan M. Ernst (#4788)
1204 N. King Street
Wilmington, DE 19801
(302) 830-4600
rernst@bk-legal.com

LEVI & KORSINSKY, LLP
Gregory M. Nespole
Daniel Tepper
Correy A. Suk
Sidharth Kakkar
33 Whitehall Street, 17th Floor
New York, NY 10004
T. 212.363.7500
F. 212.363.7171
gnespole@zlk.com
dtepper@zlk.com
csuk@zlk.com
skakkar@zlk.com

Counsel for Plaintiff